Sicurezza nel cloud
Guida all'acquisto

Forcepoint

Brochure

In questa brochure:

Criteri di valutazione: che cosa cercare in una soluzione

Come per qualsiasi tecnologia, i fornitori dei servizi di sicurezza nel cloud pubblicizzano un'ampia gamma di caratteristiche e funzionalità. Spesso è difficile distinguere tra cosa è degno di attenzione e cosa non lo è. Qui di seguito sono riportati 15 punti da tenere a mente quando valuti delle soluzioni, in modo da fare la scelta migliore per la tua azienda.

Assistenza e servizi

Che tu intenda migliorare le prestazioni di Office 365 nelle filiali, tutelare l'uso dei contenuti web da parte dei dipendenti mentre lavorano in remoto o proteggere l'uso delle app e dei dati cloud, la possibilità di avere le giuste soluzioni con il giusto team fa la differenza. Non accontentarti di un mosaico di prodotti mirati di diversi fornitori. Cerca dei partner in grado di fornirti connettività integrata e soluzioni di sicurezza facili da implementare e con un servizio di assistenza efficace.

Facilità d'uso

Non molto tempo fa i prodotti "enterprise" furono progettati per esperti secondo i quali la complessità era motivo di vanto. Oggi, nessuna organizzazione IT ha il tempo o il personale da dedicare ai prodotti distribuiti che ostacolano l'efficienza delle operazioni. Sebbene alcune soluzioni possano sembrare veloci da installare e utilizzare, soprattutto durante una demo, considera con attenzione i requisiti di implementazione in un contesto aziendale reale. È quello il contesto che assorbirà la maggior parte del tuo tempo e che avrà il massimo impatto sull'organizzazione.

Prezzi

La sicurezza nel cloud può andare da semplici firewall a complesse soluzioni integrate per la prevenzione dalle intrusioni di rete, per la sicurezza web e il controllo delle applicazioni cloud con protezione dei dati, distribuite su 1.000 siti diversi. È necessario cercare soluzioni che abbiano un prezzo chiaro e senza costi supplementari per ogni minima variazione. I contratti di licenza d'impresa possono semplificare ulteriormente la questione, offrendo tecnologie fruibili in base alle esigenze, con un unico canone per utente.

Facilità di implementazione

La capacità di integrarsi con l'ambiente esistente è fondamentale. I firewall, i gateway web e i broker di sicurezza delle applicazioni cloud devono essere tutti in grado di utilizzare l'infrastruttura esistente per estrarre informazioni sull'identità da Active Directory o inviare dati di log al SIEM. Altrettanto essenziale è la facilità con cui è possibile creare policy di sicurezza che implementino i processi aziendali reali. Considera la rapidità con cui puoi aggiungere o aggiornare le policy in centinaia o migliaia di siti. Anche se la tua organizzazione non è ancora così vasta, i sistemi concepiti per essere presenti su scala globale possono contribuire alla sua espansione e offrire ai tuoi team operativi la libertà di concentrarsi sulla crescita del business.

Personalizzazione/flessibilità

Non esistono due organizzazioni uguali e una sola soluzione non può andare bene per tutti. Anche se sicuramente avrai adottato delle policy di sicurezza generali, è probabile che vi siano aggiunte e deroghe a quasi tutti i livelli aziendali e per ogni sede, ruolo e funzione. Assicurati che le soluzioni valutate rispondano alle tue esigenze specifiche, che si tratti di limitare selettivamente l'accesso a varie parti della rete, di sorvegliare l'uso di diversi tipi di contenuti sul web o di controllare il modo in cui vengono utilizzati app cloud e dati personalizzati.

Connettività direct-to-cloud

Le iniziative di trasformazione digitale spesso cominciano con l'adozione di soluzioni SaaS (Software As A Service) in cloud, utilizzabili ovunque, che vanno a sostituire le applicazioni ospitate internamente. Tuttavia, molte reti tradizionali hub-and-spoke, specialmente quelle basate su MPLS, non sempre riescono a tenere il passo. Inoltre, si sovraccaricano facilmente e possono comportare costi di aggiornamento elevati. Ecco perché le organizzazioni di tutto il mondo stanno collegando i loro uffici e le filiali direttamente al cloud, utilizzando collegamenti internet locali a banda larga, gestiti da una rete geografica estesa definita da software (SD-WAN). Questo approccio alla connettività può ridurre drasticamente i costi di rete, migliorare la produttività degli utenti (soprattutto per le moderne applicazioni cloud come Office 365) e ridurre gli oneri operativi. Ricorda, però, che, anche se le soluzioni SD-WAN in genere integrano la crittografia per la protezione dei dati inviati, questa è soltanto la metà dell'equazione.

Uso sicuro della SD-WAN

L'utilizzo della SD-WAN per collegare i siti direttamente al cloud, invece di effettuare il backhauling del traffico verso gateway di sicurezza centralizzati, richiede un nuovo approccio alla sicurezza. È necessario tenere gli intrusi fuori dai siti remoti, ad esempio con dispositivi firewall o firewall come servizio (FWaaS), e proteggere le attività dei dipendenti su internet. Ciò include la salvaguardia dell'uso dei contenuti web (di solito tramite servizi di sicurezza web basati sul cloud) e la protezione di applicazioni e dati cloud per prevenirne l'uso improprio o l'esposizione (comunemente affidata ai CASB). Per ridurre il numero di prodotti e di fornitori, cerca soluzioni che integrino la sicurezza SD-WAN e delle filiali (spesso denominata Secure SD-WAN) insieme alla sicurezza web e al controllo degli accessi nel cloud.

Visibilità

La sicurezza non è mai una questione semplice. Le persone utilizzano dispositivi gestiti e non gestiti, app autorizzate e sconosciute. Gli eventi si verificano sempre nelle "zone grigie". Per mantenere il controllo globale, i team operativi devono essere in grado di capire rapidamente che cosa accade in tutta l'azienda. È necessario cercare delle soluzioni che vadano oltre i registri dei dati. Le dashboard interattive ti aiutano con una rappresentazione visiva rapida degli eventi che ti permette di concentrare l'attenzione sulle informazioni utili (e non sui dati) in modo da adattare le tecnologie alle tue esigenze e non viceversa.

Accesso sicuro alle applicazioni interne

Il passaggio allo smart working ha sottolineato le difficoltà da superare riguardo all'accesso alle app interne. Con riluttanza si è fatto affidamento sulle VPN, i cui costi e la cui complessità limitano la scalabilità e spesso lasciano esposte le reti. Fortunatamente esistono nuovi approcci, ad esempio le soluzioni Zero Trust Network Access che forniscono accesso privato su internet alle app interne in alternativa all'utilizzo delle VPN per utenti non amministrativi.

Protezione dei dati nel web e nel cloud

La maggior parte delle organizzazioni protegge già i propri utenti web e cloud dalle minacce internet. Ma tenere alla larga le minacce non è sufficiente, è necessario anche proteggere i (tuoi) dati. È necessario cercare soluzioni di sicurezza web e CASB (più sono integrate, meglio è) che offrano anche una effettiva protezione dei dati di classe enterprise. In questo modo ti sarà più semplice mantenere il controllo sui dati regolamentati e la proprietà intellettuale sensibile, a prescindere da dove lavorino i dipendenti.

Scalabilità

Che la tua azienda sia una Global 2000, un'agenzia governativa di portata nazionale o una media impresa, una cosa è certa: è in costante evoluzione, in fase di crescita in alcuni settori e in crisi in altri. Quando ogni secondo conta, la capacità di automatizzare i processi chiave, ad esempio l'espansione (o la contrazione) di nuove sedi, l'aggiunta di un numero elevato di nuovi utenti o l'aggiornamento dei criteri di sicurezza in tutto il mondo, diventa cruciale. È necessario cercare soluzioni concepite per gestire la complessità delle operazioni globali. Questo tipo di efficienza ti consentirà di concentrarti sulla crescita dell'azienda, anche se non è una multinazionale.

Riconoscimento/Credibilità

L'adozione delle tecnologie è un processo ciclico caratterizzato da diverse fasi: in un primo momento, le soluzioni ottengono premi e riconoscimenti per le loro funzionalità e per le caratteristiche che le distinguono dalle altre offerte presenti sul mercato. Dopo, però, l'attenzione si sposta sulle opinioni dei clienti. Osserva chi utilizza la soluzione e a quale scopo: questa considerazione ti aiuterà a trovare più rapidamente le tecnologie e le persone più adatte alle tue specifiche esigenze.

Performance secondo gli analisti

I report di analisti come Gartner Magic Quadrant e Forrester Waves e i test sui prodotti, ad esempio quelli eseguiti dagli NSS Labs, sono spesso un buon punto di partenza per trovare delle soluzioni. Ma poiché analisti diversi e test diversi arrivano sempre a risultati diversi, anche quando esaminano una stessa soluzione, piuttosto che concentrarti sulle classifiche assolute, osserva i quesiti posti e il modo in cui vengono esposte le valutazioni. In questo modo ti sarà più semplice individuare gli elementi di maggior rilievo per te.

Ambienti IT ibridi

Uno dei tratti distintivi di una soluzione completa per la sicurezza del cloud è che l'uso del cloud viene protetto a partire dal cloud stesso. Nella nostra realtà, però, in cui le applicazioni sono ovunque, sia in più cloud che on-premise, esistono molte situazioni in cui è necessario adottare localmente misure di protezione specifiche: che si tratti di semplificare la conformità o di soddisfare i requisiti di sovranità dei dati, i moderni ambienti IT aziendali sono di natura ibrida. La sicurezza deve essere laddove si trovano le risorse umane e i dati della tua azienda. Che cosa significa? Che probabilmente le soluzioni di sicurezza ibride svolgeranno un ruolo importante per proteggere la sicurezza della tua azienda e soddisfare le aspettative degli auditor.

Innovazione

Uno dei fattori più importanti da considerare in un fornitore di soluzioni è la sua motivazione: sta cercando di realizzare una vendita rapida e passare oltre o sta gettando le basi per una partnership a lungo termine? È importante osservare la sua visione della sicurezza informatica, e comprendere se è concentrato sulle principali tendenze del settore, ad esempio l'uso dell'intelligenza comportamentale e i nuovi approcci come il Secure Access Service Edge (SASE) di Gartner e i modelli Zero Trust di Forrester. In definitiva, i partner migliori si affiancheranno a te per personalizzare le loro innovazioni e rendere la tua azienda più produttiva, più efficiente e più sicura, spianandoti la strada verso successo.

Le tue opzioni a colpo d'occhio

	FORCEPOINT	ZSCALER	SYMANTEC	PALO ALTO	FORTINET	CISCO	NETSKOPE
Sicurezza su web	●	●	●	○	○	●	○
SD- WAN Direct-to-cloud	●	—	—	—	●	●	—
NGFW	●	○	—	●	●	●	○
CASB	●	○	●	○	●	○	●
Sicurezza e-mail	●	—	●	—	—	●	—
DLP per applicazioni cloud	●	—	●	—	—	—	●
Implementazione ibrida	●	○	●	○	—	●	○
RBI	●	●	●	—	—	—	—
Protezione di dispositivi non gestiti	○	○	○	○	○	○	○
Passaggio alla Behavior based Security	●	—	—	○	—	—	—

● = presente ○ = presente in parte — = presente in minima parte/assente

Zscaler – Nata come gateway web basato su cloud, Zscaler si è espansa, con l'aggiunta di nuove funzionalità come il firewall di base, alcuni CASB e, recentemente, l'isolamento del browser remoto (RBI). L'azienda sostiene in modo categorico di essere già una soluzione SASE (Secure Access Service Edge), anche se per gli analisti di Gartner non esistono ancora dei veri e propri prodotti SASE.

Symantec (Bluecoat) – Symantec offre un'ampia gamma di soluzioni di sicurezza, dai dispositivi di sicurezza web e servizi cloud, DLP e CASB alla sicurezza e-mail. Tuttavia, non offre NGFW, ponendo un limite alla visibilità e al controllo che è in grado di fornire all'interno della rete. Dopo la sua acquisizione da parte di Broadcom, Symantec ha deciso di concentrarsi esclusivamente sulle Global 2000, lasciando alle altre aziende e medie imprese il compito di trovare soluzioni alternative.

Palo Alto Networks – Nata come fornitore di prodotti firewall di "nuova generazione", la Palo Alto Networks si è espansa attraverso delle acquisizioni, trasformandosi in azienda fornitrice di una piattaforma di sicurezza. Nel 2019, ha acquisito una tecnologia di intelligence comportamentale e probabilmente tenterà di seguire le orme di Forcepoint per offrire una sicurezza basata sul comportamento. L'azienda sta perseguendo una soluzione SASE con il prodotto Prisma.

Fortinet – Originariamente nata come fornitore low-cost di firewall di nuova generazione, Fortinet ha ampliato il suo business grazie alle acquisizioni, ma è ancora nota per la mancanza di gestibilità su larga scala e l'offerta di funzionalità che non sono necessariamente combinabili.

Cisco – In quanto società di networking in posizione dominante, Cisco ha conquistato un'ampia fetta del mercato della sicurezza con un'accoppiata vincente: ha abbinato i prodotti di sicurezza alle vendite dei suoi sistemi di networking I suoi prodotti di sicurezza spesso non sono combinabili e la società è stata più volte criticata per non essere in grado di offrire ai clienti una soluzione chiara e concreta. Sta perseguendo una soluzione SASE con il prodotto Umbrella.

Netskope – Nata come fornitore di prodotti mirati CASB, Netskope offre una solida soluzione di protezione dei dati per le applicazioni cloud. Recentemente ha ampliato la sua offerta per includere la sicurezza web e aggiungerà ulteriori funzionalità per il conseguimento della SASE.

Esempi di domande da evidenziare nelle RFP

Quando prendono in esame i prodotti di sicurezza nel cloud, molte aziende trovano utile chiedere suggerimenti ai fornitore durante la fase iniziale o precisazioni durante le fasi successive. Tali Richieste di informazioni (RFI) o Richieste di proposte (RFP) possono mettere in luce funzionalità chiave in grado di definire le modalità con cui vengono utilizzati i prodotti o le soluzioni.

Se le RFP complete spesso includono centinaia di domande, qui di seguito riportiamo alcuni esempi di quesiti che potrebbero essere utili:

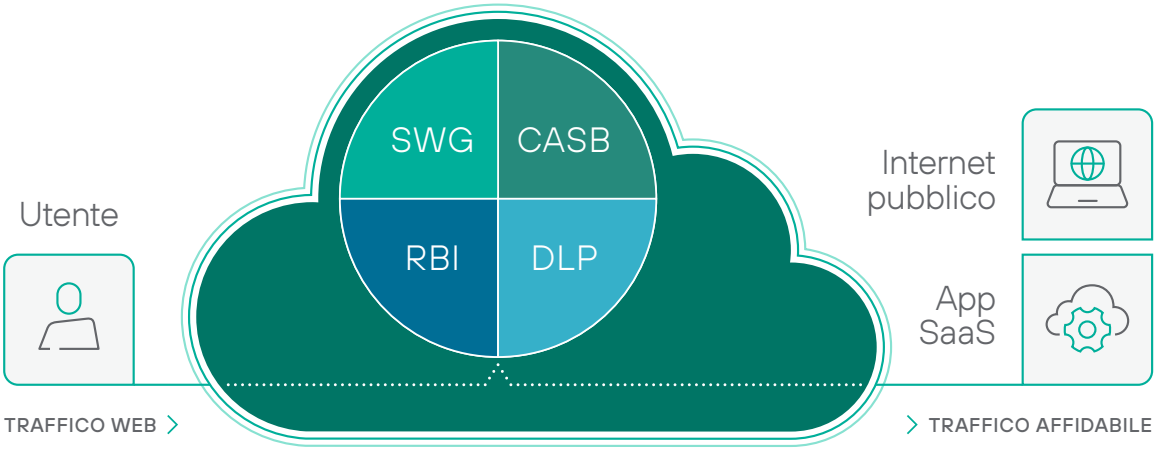
In che modo i siti e gli utenti possono connettersi alla soluzione?

DOMANDE	INFORMAZIONI CHE PUOI RICAVARE DA QUESTA DOMANDA
In che modo è implementata la soluzione (come servizio cloud, dispositivo in locale, un ibrido dei due)?	Alcune soluzioni ti costringono ad adottare un approccio indifferenziato: solo cloud o solo dispositivo. Tuttavia, la maggior parte delle aziende usa un mix di applicazioni, basate su cloud e su data center, che possono avere requisiti di sicurezza differenti. Gli approcci ibridi, nei quali l'implementazione può avvenire nel cloud come anche in locale, possono essere la risposta per i requisiti di implementazione locale di siti specifici (per sovranità dei dati o audit di conformità).
Come si connettono i siti remoti alla soluzione (da VPN a un hub centrale, GRE standard di settore, IPsec verso il servizio cloud, ecc.)?	Le soluzioni moderne agevolano la connessione diretta di ogni sito al cloud senza bisogno di configurare complicate VPN o complessi tunneling.
Come si connettono alla soluzione gli utenti in roaming (da VPN a un hub centrale, file proxy manuali, agente automatizzato)?	La sicurezza dovrebbe seguire gli utenti ogni volta che escono dalla rete aziendale (negli hotel, in visita ai clienti, ecc.) senza bisogno di meccanismi manuali o lenti come la riconnessione attraverso un ufficio centrale.
In che modo rimangono protetti gli utenti in roaming che si trovano al di qua delle difese di altre organizzazioni (ad esempio, negli alberghi, in altre aziende, ecc.)?	Le soluzioni di sicurezza che non sono progettate per gli utenti in roaming spesso interrompono la connessione o richiedono la connessione manuale su VPN quando gli utenti si trovano in luoghi che applicano controlli di sicurezza diversi.
La soluzione include la connettività SD-WAN per siti remoti o devi richiederla a un altro fornitore?	La richiesta di prodotti o servizi separati per SD-WAN, in particolare di altri fornitori, può comportare difficoltà e costi aggiuntivi.
La soluzione è in grado di fornire la localizzazione dei contenuti per ciascun utente ovunque si trovi?	In molte soluzioni di sicurezza, i contenuti web sono disponibili soltanto nella lingua del paese in cui è in funzione il servizio di sicurezza e non nella lingua del paese in cui l'utente si trova in realtà.
Il fornitore è in grado di offrire un throughput sufficiente per supportare i tipi di applicazioni da utilizzare?	Alcuni fornitori non hanno la flessibilità necessaria per ampliare la larghezza di banda offerta a ciascun cliente.

Quali controlli sono previsti per proteggere l'uso di siti web e contenuti?

DOMANDE	INFORMAZIONI CHE PUOI RICAVARE DA QUESTA DOMANDA
Quante sono le categorie di siti web che la soluzione distingue automaticamente? È in grado di categorizzare siti nuovi o sconosciuti in tempo reale?	La categorizzazione automatica dei siti web semplifica notevolmente le operazioni ed è fondamentale per proteggere o controllare l'accesso a siti web completamente sconosciuti.
A che livello di granularità è possibile controllare l'accesso ai siti e alle categorie (tempi, quote, utenti/gruppi, ecc.)?	Alcune soluzioni adottano un approccio "tutto o niente" per consentire o bloccare le connessioni. Se vuoi maggiore flessibilità, cerca un accesso controllato ai siti web che non vuoi bloccare completamente o limita i controlli a gruppi specifici di utenti.
Come vengono decriptati e ispezionati i siti criptati (SSL/TLS) salvaguardando al contempo la privacy degli utenti? Il processo è automatico o manuale?	Ora che la maggior parte degli accessi al web sono criptati, la possibilità di ispezionare i contenuti di tali siti è fondamentale. Tuttavia, molte organizzazioni adottano dei criteri rigidi contro la decriptazione dei dati personali degli utenti ricevuti da banche, fornitori di servizi sanitari e altri siti simili. L'automazione è di fondamentale importanza per proteggere la privacy degli utenti.
Le applicazioni interne sono accessibili dagli utenti remoti senza una VPN?	La maggior parte delle organizzazioni dispone ancora di applicazioni che non sono direttamente accessibili da internet, in data center interni o enclavi cloud isolate. Le nuove funzionalità ZTNA (Zero Trust Network Access) forniscono accesso privato alle app interne in trasparenza, senza le complessità delle VPN.
È possibile utilizzare la tecnologia Remote Browser Isolation (RBI) per isolare l'uso di determinate categorie di siti web?	Anziché bloccare l'accesso a siti sconosciuti o eventualmente sospetti, l'RBI consente agli utenti di vedere le informazioni senza mettere a rischio il proprio computer o la rete aziendale.
Quali tipi di controlli per la prevenzione della perdita di dati (DLP) sono previsti per proteggere gli upload sui siti web?	Una delle maggiori differenze tra le varie soluzioni di sicurezza è la gamma di filtri previsti per i file che vengono caricati sui siti web. Spesso eseguita sia nel cloud che sull'endpoint, una DLP completa e automatizzata è fondamentale per prevenire il furto o la perdita accidentale di dati.
Quali sono i tipi di sandboxing per la protezione da minacce zero-day o sconosciute forniti dalla soluzione (come l'emulazione di applicazioni/SO/CPU)?	Per difendersi dalle minacce avanzate come rootkit o attacchi che rilevano e aggirano i comuni prodotti di emulazione, è necessaria un'emulazione più avanzata.
Quale ruolo avranno i nuovi approcci alla sicurezza, come l'intelligence comportamentale e la Zero Trust, nelle versioni future?	I vecchi modelli statici con cui i criteri di sicurezza venivano applicati manualmente in un'ampia gamma di condizioni stanno lasciando il passo a nuove forme di automazione che adattano le policy alle azioni dei singoli utenti. Ciò migliorerà notevolmente l'efficacia e l'efficienza dei sistemi di sicurezza aziendali.
Quale sarà il ruolo di SASE e Zero Trust?	Proprio come i diversi "stack" di sicurezza del passato sono stati integrati nei più completi prodotti moderni, la connettività e la sicurezza stanno convergendo nel cloud per consentire alle organizzazioni di lavorare in modo molto più efficiente.

La nostra realtà rovesciata e la differenza di Forcepoint



La trasformazione digitale sta portando enormi cambiamenti nelle imprese moderne. Un tempo persone, applicazioni e dati operavano o si connettevano restando al di qua dei gateway di sicurezza. In questo modo si creava una barriera, un perimetro, che isolava i sistemi aziendali dal resto del mondo. Il mondo, però, ha subito diversi cambiamenti importanti:

Persone

Le organizzazioni stanno diventando sempre più distribuite, spesso con filiali sparse e persone che lavorano in tutto il mondo.

App/Dati

Molte applicazioni e molti dati sono stati spostati nel cloud.

Connettività

Naturalmente anche la connettività tra persone, applicazioni e dati si è spostata nel cloud.

In sostanza, l'impresa moderna si sta rovesciando. La maggior parte delle sue attività, le informazioni e le transazioni fondamentali si svolgono all'esterno del perimetro, al di là delle mura di sicurezza dietro cui è rimasta barricata per molto tempo. Qualcosa DEVE cambiare.

Le strategie di sicurezza funzionano soltanto in prossimità dell'oggetto da proteggere. Una sicurezza che segue le persone, le applicazioni, i dati e la connettività nel cloud permette alle organizzazioni di trarre realmente vantaggio dalla loro presenza nel cloud (più produttività, meno costi), di gestire i rischi e restare conformi alle leggi sulla privacy in continua evoluzione.

Oltre a essere un termine in voga, la trasformazione digitale è una delle più grandi rivoluzioni nella storia dell'informatica. Il modo in cui viene realizzata la protezione perimetrale sta subendo una cambiamento epocale. Le tecnologie sono convergenti e le aspettative tradizionali stanno mutando radicalmente.

Aziende di tutto il mondo si affidano alle competenze uniche e alle funzionalità esclusive di Forcepoint per connettere e proteggere imprese altamente distribuite e agenzie governative. Siamo l'unico fornitore in grado di offrire una soluzione di difesa verticale e orizzontale e stiamo guidando il settore verso una nuova generazione di automazione della sicurezza basata sul comportamento.

Perché le soluzioni per la sicurezza perimetrale di Forcepoint sono differenti

Portata della sicurezza
Sicurezza di web, rete, app e dati in un'unica soluzione

Ibridismo profondo
Visibilità e controllo su cloud, rete, endpoint

Risk-Adaptive Protection
Applicazione automatizzata basata sull'intelligenza comportamentale (in arrivo)

Introduzione a Forcepoint: caratteristiche e vantaggi delle nostre offerte

1. **Soluzione convergente single-vendor –** Piattaforma di sicurezza perimetrale e cloud per aziende. Include connettività di rete (SD-WAN, VPN), sicurezza di rete (NGFW), sicurezza di accesso al web e al cloud con la protezione dalle minacce e la prevenzione della perdita dei dati (Cloud Security Gateway).
2. **Scalabilità globale –** Utilizzata da aziende di tutte le dimensioni, in tutto il mondo.
3. **Implementazione ibrida –** Visibilità e controllo su cloud, rete, endpoint.
4. **Sicurezza behavior-centric –** La comprensione del contesto in cui agiscono gli utenti sugli endpoint (ad esempio capire quali programmi e quali utenti usano quali risorse nella rete) e la ricca analisi comportamentale degli utenti e delle entità (UEBA) caratterizzano un nuovo stile di automazione. Grazie alla triangolazione delle azioni a livello di singolo utente e alla raccolta di informazioni più precise su ciò che accade ovunque, la sicurezza è trasparente agli utenti fino a quando non è richiesto un intervento.
5. **SASE e Zero Trust –** Le tecnologie di protezione Forcepoint si distinguono per l'ampiezza e la profondità del loro raggio d'azione, una caratteristica esclusiva grazie alla quale potremo mettere a punto una nuova generazione di soluzioni di sicurezza che semplificheranno in modo sostanziale la tutela di dati e proprietà intellettuale.

Quali sono i vantaggi

Maggiore produttività – Performance più rapide per le app cloud moderne e più flessibilità per l'apertura di nuove sedi

Costi inferiori – Meno dispositivi e console da acquistare e gestire e spese operative più basse

Rischio ridotto – Maggiore sicurezza, comprensiva di un percorso di sicurezza behavior-centric, scalabile per crescere con le esigenze dei clienti

Conformità semplificata – Visibilità e controllo unificati su cloud, rete ed endpoint per accelerare la risposta e la remediation degli eventi imprevisti

Vuoi scoprire di più sulla soluzione convergente di sicurezza perimetrale e cloud studiata da Forcepoint per le aziende? E su come può proteggere i tuoi utenti e i tuoi dati e, allo stesso tempo, soddisfare i requisiti operativi?

Contatta uno dei nostri esperti per discutere delle tue esigenze specifiche.

Forcepoint

forcepoint.com/contact

Informazioni su Forcepoint

Forcepoint è l'azienda leader nel settore della sicurezza informatica per la protezione degli utenti e dei dati. La sua missione è tutelare le aziende e guidare la crescita e la trasformazione digitale. Le soluzioni armonizzate di Forcepoint si adattano in tempo reale al modo in cui le persone interagiscono con i dati, forniscono un accesso sicuro e, allo stesso tempo, consentono ai dipendenti di creare valore. Dalla sua sede ad Austin, Texas, Forcepoint crea ambienti sicuri e affidabili per migliaia di clienti in tutto il mondo.

[Cloud-Security-A-Buyers-Guide-Brochure-IT] 21luglio2020