Guida aziendale agli elementi essenziali per la sicurezza nel cloud

Forcepoint

Brochure

In questa brochure:

Panoramica: sicurezza nel cloud e migrazione al cloud

Se ti sembra che il cloud si diffonda sempre più, hai visto giusto.
Quali sono i motivi di questa rapida e frenetica accelerazione verso tutto ciò che è cloud?
In realtà è il consumismo, secondo il modello B2C.

Le modalità con cui si fa uso del cloud ogni giorno determinano il modo in cui le aziende adottano e proteggono il cloud.

La sicurezza nel cloud è pilotata dalle persone.

Cloud significa accesso immediato.

Il cloud rappresenta un'aspettativa.

Con l'accesso costante a contenuti, app e dispositivi, in totale trasparenza, in ogni momento e senza interruzioni, il cloud è parte integrante della nostra vita quotidiana. Profondamente intrecciato nel tessuto delle funzioni e azioni inconsce dell'uomo moderno. Anche sul posto di lavoro, l'aspettativa è la stessa: vogliamo usare ciò che serve, quando ci serve. E vogliamo un'esperienza fluida che non ostacoli, ma anzi favorisca la produttività. Com'è possibile incrementare la produttività tramite il cloud? Come si può fare di più con meno? Perché, diciamolo, cloud significa praticità, ma è anche sinonimo di vulnerabilità.

In ultima analisi una persona che lavora è una persona che consuma. Il modo in cui le aziende tutelano le loro organizzazioni, proteggendo dati e persone, deve essere all'altezza della stessa aspettativa e della stessa esperienza che caratterizzano il nostro quotidiano. E la sicurezza deve evolversi per consentire tale fluidità e, al contempo, garantire la protezione dalle minacce in continua espansione che accompagnano tale libertà e convenienza.

Questa è la cultura generale del cloud. Ma quali sono le circostanze specifiche che incitano all'azione e spingono le aziende a rivedere l'approccio al cloud e alla sicurezza nel suo complesso? Tra queste circostanze figurano:

- Il percorso della trasformazione digitale, cominciato con l'adozione e l'implementazione di O365
- Lo spostamento di app legacy e personalizzate nel cloud, come i sistemi EHR o ERP
- Persone che lavorano oltre i confini di un ufficio, fuori dalla rete aziendale o protette da altre difese
- Le imprese globali, operanti all'interno e tra ambienti altamente distribuiti, comprendono siti che necessitano dello stesso livello di sicurezza della sede centrale, senza bisogno di ricreare una costosa e massiccia presenza hardware in ogni sede con il backhauling del traffico
- Gli sforzi di ottimizzazione, volti al consolidamento degli stack di sicurezza, all'ottimizzazione dei flussi di lavoro dei team o semplicemente alla riduzione di CapEx/OpEx
- Lo spostamento delle infrastrutture verso cloud pubblici come AWS o Azure

Il modo giusto per passare al cloud

Il concetto di sicurezza nel cloud è diverso da persona a persona e cambia in modo rapido e costante. Com'è possibile tenere il passo? Come puoi essere sicuro che il tuo approccio sia olistico ed efficace? Per proteggere con successo la tua organizzazione, la sicurezza nel cloud deve essere inclusiva.

Pensiamo ai componenti fondamentali del cloud:

Dati nel cloud | **Utenti** nel cloud | **Applicazioni** nel cloud | **Connettività** nel cloud | **Infrastruttura** nel cloud | **Sicurezza** nel cloud

In sostanza, questi sono gli elementi essenziali della sicurezza nel cloud. Tutti i componenti del cloud devono essere presi in considerazione, controllati e protetti al fine di evitare falle nella sicurezza e mantenere al sicuro utenti e dati. Se il concetto di sicurezza nel cloud non ha una definizione statica, esiste, invece, un modo giusto per passare al cloud.

Qual è questo modo?

Per connettersi al cloud in sicurezza, le organizzazioni devono:

- Proteggere l'accesso ai contenuti web e alle app cloud per tutti gli utenti, ovunque e su qualsiasi dispositivo
- Avere visibilità e controllo a livello aziendale, per promuovere la strategia di sicurezza nel cloud
- Proteggere i dati quando viaggiano dal/al cloud
- Consentire la connettività direct-to-cloud per utenti e siti senza backhauling
- Ottimizzare l'infrastruttura e il flusso di lavoro
- Garantire una protezione avanzata dalle minacce, compresi gli exploit zero-day

Bene, ora che sai cosa devi fare, in che modo puoi farlo? Molte organizzazioni potrebbero avere già dei prodotti in grado di eseguire alcune funzionalità chiave o diversi team responsabili di taluni elementi di sicurezza nel cloud. Ma ogni organizzazione di sicurezza vuole evitare di sovraccaricare i propri team di sicurezza, già oberati di lavoro, implementando prodotti multipunto non integrati e non comunicanti tra loro. Ciò di cui le organizzazioni hanno realmente bisogno è una soluzione unica, non un miscuglio di prodotti di svariati fornitori. Sì, esistono delle dipendenze, ad esempio il bisogno di avere visibilità a fini di controllo o la necessità di migrare la sicurezza web locale al cloud per proteggere gli utenti fuori rete. In condizioni ottimali, la sicurezza nel cloud è una soluzione unificata che copre dati, accesso al web, accesso al cloud, dati nel cloud e connettività. L'obiettivo è quello di mitigare eventuali punti critici nel team di sicurezza ed evitare lacune nella sicurezza. A tale scopo, che si avvalgano di un solo fornitore o di tre, per conseguire i risultati chiave le imprese devono garantire l'allineamento tra mezzi a disposizione, obiettivi auspicati e presenza desiderata.

Soluzioni alle problematiche del cloud

Spostare i dati nel cloud non è un'impresa da poco e se l'idea ti preoccupa, sappi che non sei il solo. Come riuscirai a tutelare la proprietà e mantenere il controllo? Riuscirai a tenere a bada le minacce? Come potrai garantire le prestazioni?

Affrontiamo alcuni dei tipici punti in questione.

Latenza

La copertura è fondamentale per ridurre la latenza. Un'ampia presenza con numerosi PoP in tutto il mondo fornirà una bassa latenza, nonché altri vantaggi in grado di incrementare la produttività, ad esempio la localizzazione dei contenuti. **Le reti Tier 1 e i data center Tier 4** contribuiscono a garantire un'ampia portata, ridondanza, connettività e qualità, tutte caratteristiche ideali per le applicazioni sensibili alla latenza.

Visibilità

Non puoi proteggere ciò che non vedi. E non puoi apportare modifiche o stabilire dei criteri se ne ignori le conseguenze. L'abbinamento di un **gateway web basato su cloud** con un **firewall** offre una visibilità e un'implementazione coerenti tra utenti e sedi, ivi compresi l'attuazione delle policy e il controllo dell'IT shadow. E la funzionalità **CASB** aiuta a proteggere le aziende, offrendo visibilità sulle attività che gli utenti di app autorizzate e non autorizzate svolgono nel cloud, in modo da chiarire quali sono i rischi e proteggere utenti e dati.

Compliance

Affidati alle certificazioni ufficiali, non solo alla conformità auto verificata. Gli standard rilevanti per la tua organizzazione includono probabilmente:

- **ISO 27018**, in merito alle informazioni di identificazione personale (PII)
- **ISO 27001**, certificazione multisito per lo sviluppo, la garanzia di qualità, l'implementazione e le operazioni di supporto
- **CSA**, che disciplina la sicurezza del software e le operazioni interfunzionali in un ambiente cloud (e si basa sul Codice di Condotta GDPR)
- **SOC2**, incentrato sui controlli di reportistica di carattere non finanziario relativi a sicurezza, disponibilità, integrità del trattamento, riservatezza e privacy, in aggiunta a test dei data center ed efficacia operativa

Sovranità dei dati

Nonostante il cloud non abbia confini fisici, deve comunque rispettare le leggi in base ai confini e alle frontiere geografiche. I dati digitali sono soggetti alle leggi del paese in cui risiedono. L'utilizzo **di data center cloud ubicati nelle regioni in cui opera la tua azienda** è essenziale per garantire la conformità alle leggi e alle normative locali, nonché le prestazioni.

Perdita di dati

Un approccio unificato è garanzia di maggior successo. Grazie alle **soluzioni di protezione dei dati**integrate, le misure di sicurezza locali possono essere estese al web, all'e-mail, agli endpoint, alla rete e al cloud. Sfrutta le tue policy esistenti per proteggere i dati archiviati nel cloud e quelli in transito.

BYOD

La forza lavoro di oggi si basa su numerose applicazioni cloud autorizzate e non autorizzate, sia su dispositivi gestiti che non gestiti. Per mettere in sicurezza gli utenti remoti e in roaming, le difese perimetrali della rete e la protezione degli endpoint non sono sufficienti. È necessario distinguere tra dispositivi gestiti e BYOD, utilizzando **policy di sicurezza granulari** che offrano ai dipendenti la flessibilità di utilizzare i loro dispositivi senza incorrere in rischi aggiuntivi. **I controlli estesi** offrono sicurezza agli utenti remoti che utilizzano i dispositivi aziendali sia per lavoro che per uso personale.

Una scelta superficiale

Pur di acquisire agilità ed efficienza nel minor tempo possibile, quando si tratta del cloud, le aziende tendono spesso a rimandare le soluzioni a "un secondo momento" non meglio definito. Ma questo atteggiamento superficiale spesso va a discapito sia della sicurezza che dell'efficacia. Ad esempio, il solo filtraggio degli URL non è sufficiente per garantire la sicurezza e una soluzione DNS ricorsiva non è in grado di sostituire un gateway web completo. Non è possibile ottenere una protezione completa con una soluzione elementare. Inoltre, un approccio minimalista fornisce una sicurezza reattiva, piuttosto che proattiva. Devi assicurarti che sia **la sicurezza che il networking operino insieme e siano parte integrante** della roadmap per la trasformazione digitale della tua azienda, affinché procedano di pari passo con gli altri obiettivi aziendali onde evitare ritardi.

La via per il successo in un mondo connesso al cloud

Abbiamo stabilito all'inizio che la sicurezza nel cloud è pilotata dalle persone. Per questo motivo deve essere incentrata sulle persone.

Grazie al cloud, **le persone diventano il nuovo perimetro.**

Oramai utenti, partner e clienti accedono ai dati della tua azienda da qualsiasi angolo del mondo; per questo motivo il muro artificiale che protegge i dati non è più sufficiente.

La sicurezza tradizionale, incentrata sulle infrastrutture, che raggruppa gli utenti attendibili all'interno e i soggetti non attendibili all'esterno, non ha più ragione di essere.

La fiducia intrinseca non può far parte dello stack di sicurezza.

E lo stack di sicurezza costituisce un elemento integrante, non secondario, della trasformazione digitale dell'azienda.

Per accelerare e proteggere questo processo, ecco alcuni principi fondamentali da tenere a mente:

Passa al cloud secondo i tuoi tempi
Roma non è stata costruita in un giorno. La migrazione al cloud non può avvenire in 24 ore. La maggior parte delle imprese opera in ambienti IT ibridi/multi-cloud e continuerà a farlo nel prossimo futuro. Verifica che il tuo gateway web sicuro disponga di opzioni di implementazione flessibili che consentano la migrazione secondo i criteri adeguati per la tua organizzazione, oggi e in futuro. In questo modo la migrazione avverrà nei modi e nei tempi giusti per te, preservando la sicurezza generale.

Estensione perimetrale
Proteggi il cloud, la rete e gli endpoint per soddisfare le mutevoli esigenze aziendali. Una piattaforma convergente con hardware ridotto e funzionalità di sicurezza modulari offre alle organizzazioni altamente distribuite la scalabilità e la flessibilità di cui hanno bisogno per approfittare delle novità, prevenire i punti ciechi e collegare le varie postazioni in modo sicuro e gestibile.

Modello zero trust, visione totale
"Fidarsi mai, verificare sempre" è uno dei punti chiave del framework Zero Trust: per proteggere i dati dell'organizzazione è essenziale valutare l'accesso a tali dati durante l'interazione tra utente e dispositivo. Questo modello aiuta a comprendere il "chi" e il "come". Comprendere il "perché" consente di andare oltre la consapevolezza e passare alla prevenzione. Sfrutta l'analisi comportamentale per comprendere le intenzioni.

Sei pronto per il prossimo passo verso la sicurezza scalabile nel cloud?

› Consulta il nostro e-book Protezione del flusso di lavoro, ovunque e in qualsiasi momento.

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 trasformazione digitale e la crescita. 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.