radware

L'alba dell'hybrid cloud WAF

White paper

CONDIVIDI QUESTO WHITE PAPER

Indice

Perché l'hybrid cloud è così interessante?

Storicamente, le applicazioni sono il motivo per cui le aziende sono passate ad adottare sistemi autoadattanti e hanno esplorato nuove idee per penetrare il mercato. Queste "app" costituiscono dei punti cardine in cui vengono eseguite tutte le operazioni critiche. Tuttavia, è avvenuto un profondo cambiamento che ha accelerato l'evoluzione portandola a un punto di svolta: si tratta della migrazione delle applicazioni a fornitori di servizi cloud esterni. Basti pensare a quello che hanno dichiarato colossi come IBM e altri alla InterConnect Conference: il cloud non può più essere considerato né privato né pubblico, è passato a uno stato ibrido.

Per rimanere competitive e rilevanti tutte le aziende devono trasformarsi e adattarsi. Il documento analizza tre importanti motivi alla base del concetto di "cloud" come sinonimo di "ibrido".

Motivo n. 1 – La maggior parte delle aziende manterrà una parte dell'infrastruttura di application delivery internamente

Per via dei processi di business preesistenti, per aspetti legali o di compliance normativa, per riluttanza, per complicazioni dal punto di vista manageriale oppure per la perdita di visibilità del "real-time", la maggior parte delle aziende non potrà eliminare completamente l'infrastruttura IT e fare affidamento solo sul cloud. Gran parte delle aziende non è semplicemente in condizioni di trasferire sul cloud tutte le applicazioni, per diverse cause, quali:

- Applicazioni tecnicamente non adatte al cloud (ad esempio, applicazioni di gestione della produzione o relative a dispositivi a logica programmabile PLC);
- Applicazioni che per loro natura devono trovarsi in prossimità fisica del cliente;
- L'accesso Internet non è ancora abbastanza resiliente o robusto per i modelli di fornitura di servizi cloud (ad esempio in alcune aree geografiche dove la larghezza di banda o il QoS non sono ancora ai livelli necessari per erogare servizi Cloud con Sla accettabili);
- La conformità alle normative o alla legislazione vigente possono imporre che i dati o le applicazioni che li elaborano rimangano all'interno di una determinata area geografica o all'interno di una predeterminata ubicazione;
- Applicazioni a cui si accede internamente (intranet, non pubblicamente accessibile);
- Applicazioni con utilizzo intensivo di dati che accedono a informazioni sensibili (per applicazioni che non accedono a dati sensibili l'archiviazione (storage) in cloud può offrire soluzioni economicamente convenienti, così come per le applicazioni che non fanno uso intensivo di dati e per le quali il costo dell'accesso a dati archiviati in locale in termini di overhead di traffico, non è significativo).

Molti fornitori definiscono un cloud ibrido come la combinazione di uno qualsiasi dei seguenti modelli: on premises, cloud privati e cloud pubblici. Tuttavia, è un concetto che cessa di essere rilevante quando i servizi IT sono gestiti da chi possiede l'infrastruttura sottostante: è il coordinamento di tali servizi che li rende ibridi.

Le domande da porsi quando si procede alla migrazione delle applicazioni al cloud

1. Ho sia applicazioni con accesso interno sia altre con accesso pubblico?
2. Avrò un periodo di transizione nel quale ho applicazioni sia in locale sia nel cloud?
3. Alcune applicazioni sono destinate a rimane in locale (applicazioni mission-critical o che richiedono accesso a dati sensibili archiviati internamente) a lungo termine?
4. Come proteggere sia le applicazioni in locale sia le applicazioni basate su cloud?
5. Come proteggere le app durante la transizione al cloud?
6. Trasferisco le app in un'unica infrastruttura cloud o mi rivolgo a più fornitori?
7. Come ottenere dei criteri di sicurezza controllati e gestiti per le mie applicazioni nei vari scenari menzionati sopra? Come ottenere visibilità centralizzata sulla reportistica e i criteri di sicurezza?
8. Ho visibilità sul ciclo di vita dello sviluppo dei sistemi (SDLC) e sul processo di rilascio di app? So che cosa è stato modificato? So quale può essere l'impatto sui criteri di sicurezza?
9. Ho visibilità sui differenti framework e tecnologie Web utilizzati per sviluppare ed eseguire le app Web? Sono consapevole delle varie vulnerabilità di ogni piattaforma e tecnologia?

Un approccio al cloud ibrido non richiede una migrazione completa dell'infrastruttura IT tradizionale a un cloud pubblico o privato.

Motivo n. 2 – Le infrastrutture dedicate sono un lusso che rendono gran parte delle aziende non competitive in confronto alla concorrenza che ricorre all'ibrido

Sono chiari i meriti della virtualizzazione e del cloud, che fanno emergere efficienze latenti che rimanevano inutilizzate con i data center classici. Ad esempio, quando si realizza un data center di tipo legacy, bisogna progettare e costruire un'infrastruttura IT tipica per i momenti di picco. Come dimostrato da progetti di virtualizzazione di server, l'utilizzo medio dei server fisici tende a non superare il 12-18%. Le aziende hanno cominciato a virtualizzare i server fisici per poter incrementare questo tasso di utilizzo arrivando fino al 30-40% o oltre. Ora lo stesso fenomeno si sta verificando relativamente alla virtualizzazione della rete, poiché ci troviamo in una fase caratterizzata dalla virtualizzazione delle caratteristiche di rete (NFV) e dalle reti di tipo Software Defined Network (SDN).

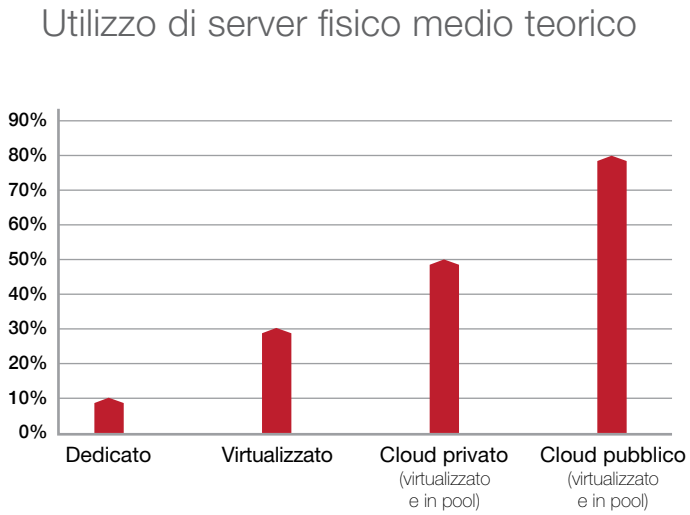

Figura 1: Utilizzo di server fisico

Il cloud per molti aspetti è stato un ulteriore tentativo di ampliare la virtualizzazione e incrementare utilizzo ed efficienza. In pratica era stato inteso come un gruppo di server virtualizzati in gruppi di risorse con portali di accesso in modalità self-service che consentono di creare, modificare ed eliminare facilmente nuovi carichi per server. Il cloud è stato progettato per liberare l'utente finale dalla complessità della virtualizzazione e consentire in modo autonomo e veloce la piena disponibilità del servizio. Ad esempio, per portare i server fisici fino a un'efficienza dell'80% si fa ricorso a un'implementazione di tipo "multi-tenancy", che spesso comporta la necessità di disporre di soluzioni cloud, per fornire servizi ad aziende diverse con picchi di carico variabili nel tempo. Molti la considerano una "oversubscription" dei server da parte di vari clienti individuali, ma questo modello può avere successo se i clienti avranno picchi di carico in momenti diversi.

Inoltre, questi sistemi cloud devono funzionare perfettamente con applicazioni e sistemi aziendali già in uso, spesso integrati sia dal punto di vista tecnico che procedurale, rendendo ibrido il modello di fornitura del servizio.

Motivo n. 3 – Sicurezza delle informazioni e conformità alle normative

La sicurezza cloud rimane non chiaramente definita. Inoltre, è considerato pratica comune il fatto che benché la tecnologia dell'informazione possa essere data in outsourcing o fornita da un fornitore terzo, lo stesso non vale per quanto riguarda la gestione della sicurezza. In altre parole, la sicurezza rimane sempre una responsabilità dell'azienda fornitrice ed è stata sempre una soluzione "ibrida" sin dagli inizi.

Dalle origini dei modelli di fornitura cloud, la sicurezza è stato un elemento portante nel ricorso a questa risorsa, per il timore di inadeguatezze e altri problemi. In generale, il cloud ha comportato la necessità di fornire la sicurezza dei sistemi informativi in tre ampie categorie.

Requisito di sicurezza cloud per la sicurezza delle applicazioni: attacchi basati su Web

La classificazione data da "The Open Web Application Security Project (OWASP) Top 10" (Open Web Application Security Project) definisce le minacce più comuni nell'ambito della sicurezza applicativa. Questa categoria di attacchi generalmente non è coperta dalle tecnologie di sicurezza tradizionali come firewall di rete e IDS (Intrusion Detection System), che sono incentrate sulle minacce relative alla rete di comunicazione e relativi vettori di attacco. Tra i vari tipi di problemi relativi alla sicurezza, le aziende avevano bisogno di fare in modo che determinate minacce (come le seguenti) fossero ben affrontate nel cloud:

- SQL Injections
- XSS (Cross-Site Scripting)
- CSRF (Cross-Site Request Forgery)
- Session Management attacks

Tuttavia, esistono molti altri vettori di attacco che minacciano le applicazioni Web in aggiunta alle Top 10 elencate dall'OWASP. La gravità di tali attacchi può dipendere dall'applicazione, e in alcuni casi possono essere dannosi. Alcuni di questi ulteriori vettori di attacco sono elencati nella classificazione delle minacce WASC.

- Brute force
- Predictable resource location
- Path traversal
- HTTP response splitting
- Abuse of Functionality

Domande da porre a un fornitore di sicurezza cloud

1. Quale tipo di soluzione potete offrire per proteggere le mie applicazioni in locale e basate su cloud?
2. Quale tipo di soluzione potete offrire per proteggere le mie applicazioni accessibili dall'interno e pubblicamente?
3. Come eviterete la generazione di falsi positivi quando l'applicazione cambia?
4. Quali tipi di attacchi sono compresi nel vostro SLA per la protezione?
5. In che modo la vostra soluzione protegge da vari attacchi Web?
   a. Caricamento di un contenuto fraudolento nell'applicazione?
   b. Manipolazione di protocollo HTTP come HTTP response splitting?
   c. Inquinamento dei parametri?
   d. Attacchi alla gestione sessioni e cookie poisoning?
6. Io (cliente), quante ore di lavoro devo investire al mese nella gestione dei criteri per assicurare che le mie app non generino dei falsi positivi?
7. Offrite consulenza per la messa a punto e la configurazione dei criteri? A quale costo aggiuntivo?

Riassumendo, la maggior parte delle aziende che stanno trasferendo le applicazioni da implementazioni interne a data center, evolvendosi quindi in direzione del cloud, si è ritrovata con meno opzioni e funzionalità disponibili con cui proteggere le applicazioni nel cloud.

Requisito di sicurezza cloud: conformità alle normative

Vari requisiti di conformità normativa hanno determinato un enorme ritardo nell'adozione del cloud, poiché tali requisiti erano spesso assenti inizialmente in questa tecnologia. Inoltre, la conformità normativa delle aziende che si occupano di erogare servizi in cloud, doveva rispondere alle richieste provenienti delle aziende clienti, per garantire che i servizi cloud fossero allineati a quanto già presente all'interno delle aziende come proprie infrastrutture in loco o su cloud privato. Ecco alcuni esempi di enormi requisiti di conformità:

- PCI-DSS (Payment Card Industry Data Security Standard)
- HIPAA (Health Insurance Portability & Accountability Act)
- Sarbanes-Oxley Act
- Patriot Act
- Varie leggi sulla privacy comunitarie e nazionali

Alla fine, c'è stato un diffuso ricorso agli "standard frameworks" per affrontare molti degli approcci tipici della sicurezza delle informazioni, nonché ai test per la valutazione di questi stessi framework. Tali framework includono SAE16 (in sostituzione di SAS70), ISO 27001 e HIPAA HiTrust.

Requisito di sicurezza cloud: problemi relativi alla disponibilità di reti di comunicazione e applicazioni, ovvero DDoS

Il compito per una azienda di tenere in funzione e con alta affidabilità i servizi IT, e al contempo gestire i vari modelli di servizi cloud utilizzati, non è banale. L'adozione del cloud si può paragonare all'adozione del Just-in-Time inventory nelle aziende manifatturiere, con tutti i relativi vantaggi in termini di costi e agilità, importanti nell'era della "affidabilità elevata". Inoltre, l'alta affidabilità non è solo una questione di contratto basata su SLA a cui sono legate penali in caso di violazioni: sta diventando cruciale per garantire la sopravvivenza e i processi operativi delle aziende. Infine, la questione dell'affidabilità ha diverse sfaccettature, poiché occorre tenere conto di numerose categorie di minacce alla sicurezza, come le seguenti:

- Attacchi volumetrici (ad esempio DDoS) Vs attacchi non volumetrici (ad esempio SQL injection che portano all'interruzione di servizio)

- Bot Vs persone. Determinare la differenza tra le attività legittime e illegittime eseguite dalle persone (come ad esempio gli hacker) era compito di tecnologie installate on premises. Ora quest'ambito si è ampliato e comprende la distinzione tra utilizzatori come persone (autorizzate o meno) e bot (o programmi automatizzati); anche questi ultimi possono essere legittimi o illegittimi.

- Esaurimento di risorse di rete
  - Saturazione di banda, spesso detta DDoS. Questo ambito ricava sovente dei vantaggi dalla transizione al cloud, poiché le aziende che erogano servizi cloud spesso hanno una larghezza di banda maggiore e migliore fattore di scala. Tuttavia, ciò non impedisce che le aziende che erogano servizi nel cloud siano immuni alla saturazione di banda Internet e spesso il rischio aumenta in ambienti multi-tenant, dove può verificarsi un effetto domino su tutte le aziende utilizzatrici dei servizi cloud.

  - Infrastruttura data center – All'interno del data center stesso vi sono molte opportunità per saturare i dispositivi di rete, bloccando il transito della tecnologia. Esempi di attacchi di questo tipo sono il superamento dei limiti sulle sessioni sui firewall, il superamento dei limiti di connessione al secondo sulle applicazioni e la saturazione in genere dei servizi quali "TCP stack resolution services".

- Tecniche di saturazione Web – Uno dei concetti meno compresi è il contributo delle vulnerabilità delle applicazioni Web all'origine dell'interruzione delle disponibilità applicative di un'azienda. Secondo il Global Application & Network Security Report 2014-2015 di Radware, il 27% di tutte le interruzioni di servizio è dovuto allo sfruttamento delle vulnerabilità delle applicazioni Web. Benché in teoria una qualsiasi delle categorie OWASP possa condurre a un problema di resilienza, le interruzioni di servizio a livello Web ruotano principalmente attorno ai cinque seguenti vettori:

  - Flood HTTP base (GET/POST) – criptati o meno
  - CDN: flood dinamici HTTP
  - Brute Force Attacks
  - Input validation attack
  - SQL/JSON/XML/LDAP Injections

  I fornitori di servizi cloud spesso non hanno le conoscenze, gli strumenti di rilevamento o tutto l'occorrente per rilevare, bloccare, o riportare tali minacce.

- Campagne di attacco multivettore. Sarebbe già abbastanza se gli attacchi elencati sopra fossero tutto ciò con cui deve confrontarsi un'organizzazione, mentre in realtà questi attacchi non si presentano mai da soli: fanno generalmente parte di quelli che oggi sono noti con il nome di attacchi multivettore. Gli attacchi multivettore si presentano sotto diverse forme. Tuttavia, secondo Global Application & Network Security Report 2014-2015 di Radware, gli attacchi raramente hanno vettori singoli e in media hanno 7 vettori differenti, che contengono almeno una delle seguenti categorie:

  - SYN flood (attacco volumetrico)
  - UDP flood (attacco volumetrico)
  - Attacchi specifici alle applicazioni (ad esempio, injection o brute force attack)
  - Attacchi criptati

- Gli attacchi multivettore sono una strategia molto efficace per chi li perpetra perché:

  - Complicano il rilevamento poiché richiedono una grande quantità di potenza di elaborazione da parte dei destinatari per individuare e correlare i vettori degli attacchi.
  - Fungono da copertura per attacchi più subdoli e spesso più penetranti.
  - Complicano le analisi forensiche e le ricerche, espondendo i punti più deboli nell'infrastruttura di difesa.

Sfide attuali per cloud WAF in ambienti ibridi

Attualmente tre macro tendenze in ambito tecnologico stanno contribuendo alla complicazione delle implementazioni e tecnologie di sicurezza delle informazioni. Queste tendenze possono inoltre entrare in collisione tra loro e rendere estremamente difficile il lavoro di chi si occupa di sicurezza delle informazioni.

La prima tendenza è il ricorso al cloud stesso. Si tratta di un fenomeno già descritto. Tuttavia, si può tranquillamente affermare che ognuno si avvale in qualche modo di varie forme di cloud. Il secondo fattore consiste nel fatto che l'Internet delle cose (IoT) sta cambiando in modo incommensurabile il numero di end point e il tipo di requisiti di accesso, ampliando il perimetro attaccabile. Infine, è in corso una rivoluzione nel modo di condurre il routing con nuovi protocolli e standard, che stanno letteralmente mettendo in discussione le best practice utilizzate per decenni.

Tendenze critiche attuali

- Migrazione cloud
- Internet delle cose (IoT)
- Virtualizzazione delle caratteristiche di rete (NFV/SDN)

Queste evoluzioni tecnologiche hanno cambiato enormemente le aspettative dei manager nei confronti dell'IT e messo in discussione molti dei modelli di sicurezza che ci si aspettava. I cambiamenti hanno comportato le seguenti complicazioni per i professionisti della sicurezza:

- Ambienti operativi differenti (ad esempio in locale, cloud, hosting, gestiti, collocati ecc.)
- Perdita di visibilità nei confronti del "panorama d'insieme"
- Aspettative elevate: ormai le aziende si aspettano che l'IT abbia tempi di reazione di ore o persino minuti in confronto a quelli che prima erano giorni o settimane. Avete bisogno di mettere online una nuova applicazione? Ci si aspetta che avvenga oggi stesso, non tra un paio di settimane. I professionisti della sicurezza si trovano spesso costretti a fare compromessi tra attuare tutti i controlli necessari per proteggere le operazioni e lasciare che l'azienda proceda alla velocità richiesta dal business, con la conseguenza che i controlli per la sicurezza avranno possibili punti deboli o lacune.
- La capacità di rilevare con efficienza le minacce in una sede e reagire a tali rilevamenti in tutti gli ambienti operativi in tempo reale.
- Redigere le giuste regole relative alla sicurezza in una sede e automatizzarle nell'intera infrastruttura IT e delle applicazioni, sia essa gestita internamente o in outsourcing.
- Coordinare le modifiche ai sistemi interessati in modo rapido e universale. Modificare manualmente tutti i dispositivi necessari può richiedere del tempo ed è un processo incline agli errori.

Fino a poco tempo fa non esisteva nessuna tecnologia di firewall per applicazioni Web che affrontasse i problemi di cui sopra. Le soluzioni offerte dai fornitori di soluzioni di sicurezza non includono un firewall per applicazioni Web che comprenda protezione sia in locale sia in cloud. Ciò costringe le aziende a integrare soluzioni di due differenti fornitori. I problemi derivanti dal ricorso a diversi fornitori, tra cui percorsi di integrazione, processi di gestione e supporto e punti ciechi (blind spots), possono comportare lacune nella copertura e nella qualità della protezione.

Questa carenza di integrazione tra la protezione in locale e nel cloud limita la visibilità sugli attacchi e su chi li perpetra nella rete. Le organizzazioni non sono in grado di distinguere gli attacchi che avvengono nel cloud da quelli che avvengono in locale. Si è trattato della stessa vulnerabilità? Il responsabile è la stessa entità per entrambi gli attacchi? Non c'è risposta definitiva a queste domande perché la qualità del rilevamento è limitata. Le organizzazioni hanno bisogno di poter affrontare sul posto e non nel cloud un problema relativo alla sicurezza.

La protezione delle applicazioni in locale, nel cloud e durante il periodo di transizione (da locale a cloud) richiede una soluzione ibrida che consente una semplice migrazione dei criteri (da locale a cloud) per eseguire in modo ottimale il trasferimento senza esporre ad attacchi Web le applicazioni appena trasferite.

Hybrid cloud WAF di Radware

Il servizio Hybrid Cloud WAF di Radware offre un servizio di firewall per applicazioni Web basato su cloud completamente gestito da Radware e sempre attivo. È il primo servizio cloud WAF ibrido che si integra con i dispositivi in locale Radware per garantire copertura completa. Il servizio offre protezione completa e senza confronti contro gli attacchi basati su applicazioni Web ed è basato sulla soluzione di prevenzione degli attacchi informatici comprendente firewall per applicazioni Web, sul dispositivo di prevenzione attacchi perimetrali e sul servizio scrubbing in cloud di Radware. Queste tecnologie operano in un'architettura basata su cloud, distribuita e scalabile, fornendo una protezione unificata senza falle di sicurezza tra dispositivi basati su locale e su cloud.

Il servizio Hybrid Cloud WAF è l'unica soluzione con le stesse tecnologie in CPE e in cloud WAF ed è fornita da un unico fornitore, con gestione e reportistica completamente integrate, per proteggere sia le applicazioni basate su cloud sia quelle in locale. Il servizio offre visibilità e controllo in ambienti di application delivery distinti per fornire rilevamento e prevenzione degli attacchi completi. Consente in tutto il mondo la prevenzione delle minacce rilevate nel cloud inviando segnalazioni ai dispositivi Radware installati in locale, nonché facilità e rapidità di coordinamento e automazione dei criteri di sicurezza.

Protezione delle applicazioni Web senza confronti

Il servizio Hybrid Cloud WAF è basato principalmente sul firewall per applicazioni Web di Radware: AppWall. È dotato di certificazione ICSA ed è l'unico WAF nel cloud a offrire copertura completa dalla Top 10 OWASP degli attacchi. Supporta modelli di sicurezza positivi e negativi e ha l'abilità unica di generare policy automaticamente.

Servizio di sicurezza completamente gestito

Include assistenza 24 ore su 24, 7 giorni su 7, revisione e analisi proattive dei log, monitoraggio di sistema e generazione di criteri automatica. Offre alle organizzazioni assistenza e servizio completi durante e dopo gli attacchi. È un servizio completamente gestito, supportato dall'Emergency Response Team (ERT) di Radware: un gruppo di esperti in materia di sicurezza che effettuano un monitoraggio attivo e prevengono gli attacchi in tempo reale.

Modello facile e flessibile

Il servizio è offerto con un modello basato su OPEX (modello ad abbonamento) semplice e composto da 3 pacchetti tra cui scegliere (Silver, Gold & Platinum). È facile da implementare e non richiede processi di impostazione né download/installazione di elementi aggiuntivi. È trasparente al servizio da proteggere. Una volta configurato, gli esperti di sicurezza Radware hanno accesso immediato ai sistemi di protezione e non hanno bisogno di alcuna interazione né risorse del cliente per l'avvio.

Protezione anti-DDoS sempre attiva

Il servizio è supportato dal dispositivo di prevenzione attacchi DefensePro di Radware, che include anti-DDoS, NBA e protezione IPS da "network and application downtime", sfruttamento delle vulnerabilità delle applicazioni, diffusione di malware, anomalie di rete, furto di informazioni e altri attacchi informatici emergenti. La protezione DDoS di Radware si avvale di moduli di rilevamento e protezione multipli comprendenti analisi comportamentale attiva, tecnologie di challenge response (sfida-risposta), oltre al rilevamento tramite firme (signature) per ridurre al minimo i falsi positivi e l'impatto sul traffico legittimo.

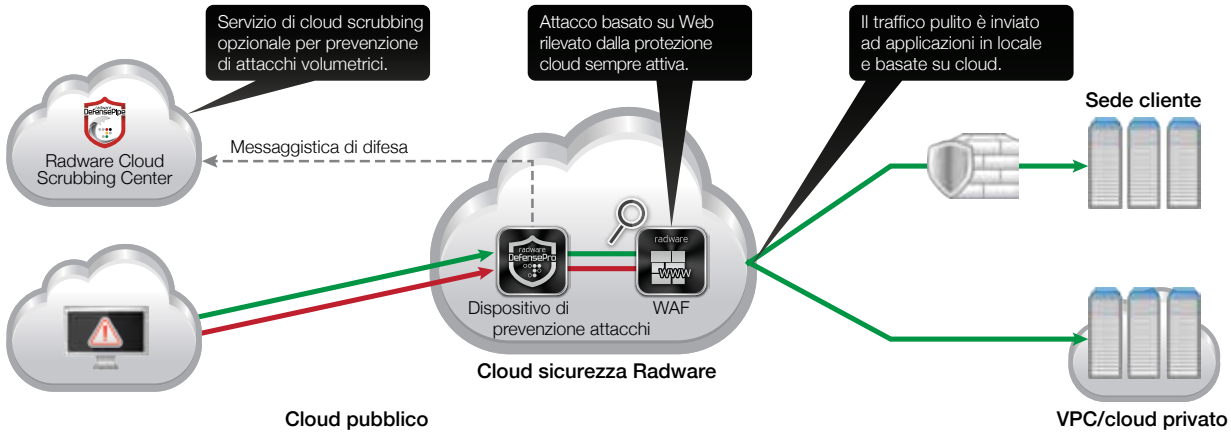

Figura 2: Prevenzione attacchi Web ibrida nel cloud

Il servizio Hybrid Cloud WAF di Radware è l'unica soluzione fornita da un unico produttore a proteggere sia le applicazioni basate su cloud sia quelle in locale. È un servizio completamente gestito che fornisce protezione senza confronti contro attacchi basati su Web e comprende copertura completa della Top 10 OWASP delle minacce nonché protezione da attacchi DDoS sempre attiva.