radware

CONDIVIDI QUESTA BROCHURE

Servizio Hybrid Cloud WAF

Il primo servizio Hybrid Cloud WAF

Un servizio sempre attivo e completamente gestito per una protezione senza pari dagli attacchi alle applicazioni Web

Migrazione sul cloud e dissolvenza del perimetro aziendale

Migrare sul cloud significa avere a disposizione un'infrastruttura di rete più distribuita. Le organizzazioni hanno bisogno di un servizio semplice, centralizzato e completamente gestito per usufruire di una protezione completa dagli attacchi basati sul web.

Molte aziende hanno spostato sul cloud per lo meno alcuni degli aspetti relativi alle proprie funzionalità IT, e le organizzazioni stanno iniziando ad adottare tecnologie cloud per migliorare l'efficienza generale ed espandere le proprie opportunità di business. I data center più virtualizzati stanno creando dei cloud privati per sfruttare al meglio le risorse aziendali.

Le imprese al giorno d'oggi non possono ignorare il risparmio e la flessibilità delle soluzioni cloud. Con una maggiore pressione sui dipartimenti IT per garantire risultati con budget minimi, la migrazione delle applicazioni e dei servizi sul cloud non si ferma. In un periodo in cui il perimetro aziendale tradizionale sta tendendo a scomparire, le organizzazioni hanno a che fare con un'infrastruttura di rete più distribuita, divisa tra i vari fornitori di servizi cloud e la rete privata dell'organizzazione. Se alcune applicazioni hanno completato la propria migrazione sul cloud, altre sono ancora in fase di transizione oppure rimarranno in sede.

Proteggere un'infrastruttura distribuita su vari livelli, specialmente dato il diverso grado di protezione offerto dai vari fornitori di servizi cloud, è una sfida ardua.

L'importanza di una soluzione ibrida

Con le attuali richieste del settore, le organizzazioni hanno bisogno di un servizio semplice, centralizzato e completamente gestito che offra una protezione completa dagli attacchi basati sul web. La soluzione deve integrare una protezione basata sul cloud con una protezione a livello locale e ricoprire un'ampia gamma di vettori d'attacco.

Le soluzioni offerte dai fornitori di servizi di sicurezza oggi non comprendono un Web Application Firewall (WAF) che garantisca una protezione locale e sul cloud contemporaneamente. Per questo l'azienda è costretta a integrare due diverse soluzioni. I problemi che sorgono dalla gestione contemporanea di soluzioni di diversi produttori, compresi il processo di gestione e di supporto, l'integrazione del piano d'azione e i punti ciechi possono portare a dei buchi nella sicurezza relativi alla copertura e alla qualità della protezione.

La mancanza di integrazione tra la protezione in sede e quella sul cloud porta a una limitata visibilità degli attacchi alla tua rete e degli aggressori. Le organizzazioni non possono differenziare gli attacchi che avvengono sul cloud da quelli che avvengono in sede. Il livello di vulnerabilità era lo stesso? Gli esecutori sono stati gli stessi per entrambi gli attacchi? Queste domande semplicemente non possono avere risposta a causa dei limiti del livello del rilevamento. Le organizzazioni devono essere in grado di prevenire un problema relativo alla sicurezza sia in sede sia nel could.

Servizio Hybrid Cloud WAF completamente gestito

Il servizio Hybrid Cloud WAF di Radware fornisce un Web Application Firewall basato sul cloud sempre attivo e completamente gestito. È il primo servizio WAF ibrido sul cloud del settore a integrarsi con i dispositivi Radware in sede per fornire una copertura totale. Il servizio offre una protezione completa e ineguagliata dagli attacchi a livello applicativo ed è basato sulla soluzione per la prevenzione degli attacchi informatici di Radware che comprende il Web Application Firewall, il dispositivo per la prevenzione degli attacchi a livello perimetrale e il cloud scrubbing. Queste tecnologie operano all'interno di una configurazione distribuita e scalabile basata sul cloud e forniscono una protezione unificata senza buchi nella sicurezza tra i dispositivi in sede e quelli basati sul cloud.

Il servizio Hybrid Cloud WAF è l'unico servizio con le tecnologie CPE e WAF sul cloud integrate e offre un'unica soluzione per proteggere sia le applicazioni in sede sia quelle basate sul cloud, con funzioni per i report e per la gestione completamente integrate. Il servizio fornisce visibilità e controllo in ambienti disomogenei di applicazioni per garantire un rilevamento e una prevenzione completi dagli attacchi. Consente una prevenzione delle minacce a livello mondiale sul cloud grazie alla comunicazione con i dispositivi di sicurezza Radware a livello locale e rende più semplici e rapide l'orchestrazione e l'automazione delle politiche sulla sicurezza.

CATEGORIE DI ATTACCO GESTITE

Terminazione e normalizzazione TCP • Protocollo HTTP (per es. HRS) • Attacchi JSON e XML	• Path traversal	• Attacchi codificati e in Base 64
Protezione dell'accesso • Password Cracking – Brute Force		
Regole per attacchi tipici • Cross Site Scripting (XSS) • Server Side Include (SSI)	• Injection: SQL, LDAP	• OS Commanding
Protezione LFI/RFI • Inclusione file locali	• Inclusione file remoti	
Protezione della sessione • Manipolazione dei cookie	• Dirottamento di sessione	
Prevenzione della fuga di informazioni • Numero carta di credito (CCN)	• Social Security (SSN)	• Espressioni regolari
Controllo degli accessi • Posizione risorse prevedibili	• Backdoor e risorse per il debug	• Attacchi agli upload dei file
Protezione DDoS • DDoS comportamentali di rete • DDoS comportamentali di applicazione	• Richiesta di conferma di rete • Richiesta di conferma HTTP	• Lista di accesso • DDoS volumetrici (add-on)

- **Protezione ineguagliata delle applicazioni web**
  Il servizio Hybrid Cloud WAF si basa principalmente sul Web Application Firewall di Radware – AppWall. Ha la certificazione ICSA Labs ed è l'unico WAF per il cloud che fornisce una prevenzione completa da tutti gli attacchi top 10 dell'OWASP. Supporta modelli di sicurezza positivi e negativi e ha l'abilità unica di generare policy automaticamente.

- **Servizio di sicurezza completamente gestito**
  Comprende un supporto 24x7, un'analisi e un controllo proattivi del registro, il monitoraggio del sistema e una generazione automatica della policy. Offre alle organizzazioni un supporto e un servizio completi prima, durante e dopo gli attacchi. Il servizio è supportato dall'Emergency Response Team (ERT) di Radware – un gruppo dedicato di esperti in materia di sicurezza che effettuano un monitoraggio attivo e prevengono gli attacchi in tempo reale.

- **Modello semplice e flessibile**
  Il servizio è presentato in un semplice modello di sottoscrizione ad abbonamento (di tipo OPEX) con 3 pacchetti tra cui scegliere (Silver, Gold & Platinum, illustrati sotto). È semplice da impostare, senza particolari processi di implementazione e senza dover scaricare/installare elementi. Dopo l'impostazione, agli esperti di sicurezza di Radware è fornito un accesso immediato e non richiedono alcuna interazione con il cliente o nessuna risorsa per iniziare il lavoro.

- **Protezione DDoS sempre attiva**
  Il servizio è supportato dal dispositivo per la prevenzione degli attacchi informatici di Radware – DefensePro – che include una protezione NBA, IPS e anti-DDoS per prevenire tempi di inattività della rete o delle applicazioni, sfruttamento delle vulnerabilità delle applicazioni, diffusione di malware, anomalie di rete, furto di informazioni e altri attacchi informatici emergenti. La protezione dagli attacchi DDoS di Radware sfrutta diversi moduli per il rilevamento e la prevenzione, tra cui un'analisi dinamica dei comportamenti e delle tecnologie con richiesta di conferma, oltre a una particolare tecnica di rilevamento per ridurre al minimo i falsi positivi e l'impatto sul traffico legittimo.

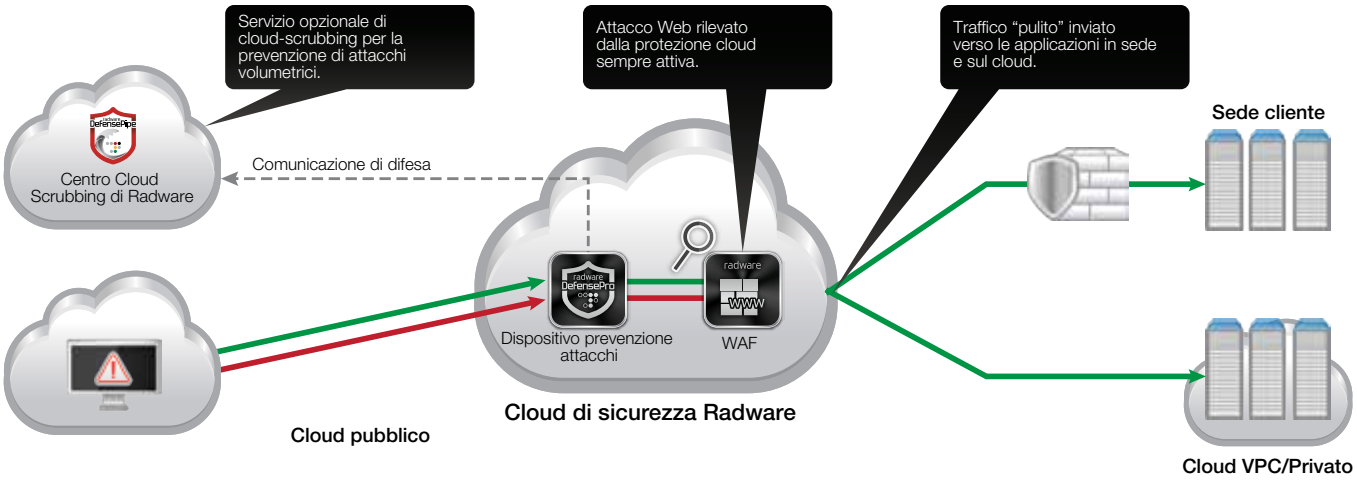

Figura 1: Prevenzione degli attacchi Web ibridi sul cloud

Offerta del servizio Cloud WAF

Il servizio Hybrid Cloud WAF di Radware è disponibile in tre pacchetti, con diversi gradi di protezione, personalizzazione e supporto.

- **Platinum** – Offre una policy per dominio, in cui la policy viene configurata per garantire, oltre alla protezione dagli attacchi fornita nei livelli Silver e Gold, anche una protezione dagli attacchi zero-day (per es. profiling dei parametri e delle pagine delle applicazioni, protezione dei cookie, configurazione XML e dei servizi Web).
- **Gold** – Offre una policy per dominio, in cui la policy viene configurata per proteggere dagli attacchi ai dati e agli accessi, oltre che dagli attacchi comuni (per es. Controllo degli accessi alle applicazioni, prevenzione della fuga di informazioni, protezione della pagina di accesso, cross-site request forgery).
- **Silver** – Offre una policy singola per cliente, configurata per proteggere dagli attacchi Web comuni (e.g. SQL injections, XSS).

In tutti i pacchetti è inclusa la protezione da attacchi DDoS fino a 1 Gbit/s di traffico legato agli attacchi. Ciò include una protezione comportamentale DDoS a livello dell'applicazione e della rete con richiesta di conferma. I clienti possono scegliere di aggiungere ulteriore banda oltre 1 Gbit/s per la protezione dagli attacchi DDoS volumetrici tramite il servizio di cloud scrubbing di Radware, che protegge la banda Internet del cliente. Il servizio è offerto in base alla somma di traffico legittimo e garantisce la protezione da un numero illimitato di attacchi al mese.

Il servizio Hybrid Cloud WAF di Radware è l'unica soluzione integrata per proteggere sia le applicazioni in sede sia quelle basate sul cloud. È un servizio completamente gestito che fornisce una protezione senza pari dagli attacchi Web, una prevenzione completa da tutti gli attacchi top 10 dell'OWASP e una protezione sempre attiva dagliattacchi DDoS.

Informazioni su Radware

Radware (NASDAQ: RDWR), è un'azienda leader a livello globale nella fornitura di soluzioni per application delivery e sicurezza delle applicazioni destinate ai data center in ambienti virtualizzati, cloud e software. L'ampia offerta di premiate soluzioni Radware garantisce la sicurezza a livello del servizio per le applicazioni aziendali "Mission Critical", portando al massimo l'efficienza IT. Grazie alle soluzioni Radware, oltre 10.000 clienti di tutto il mondo, tra aziende e operatori TLC, riescono a reagire rapidamente alle sfide del mercato, mantenere la continuità operativa aziendale e ottenere la massima produttività, contenendo contemporaneamente i costi. Per ulteriori informazioni, visitare il sito www.radware.com.

Radware favorisce la partecipazione alla propria community e consiglia di seguire l'azienda su Facebook, Google+, LinkedIn, il blog di Radware, SlideShare, Twitter, YouTube e l'app Radware Connect per iPhone®.

Scopri di più

Per avere maggiori informazioni su come le soluzioni integrate di Radware per la distribuzione e la sicurezza delle applicazioni possono aiutarti a sfruttare il massimo i tuoi investimenti aziendali e IT, inviaci un'e-mail all'indirizzo info@radware.com o vai su www.radware.com.