FORTINET®

SICUREZZA DI RETE PER IL CLOUD IN TUTTE LE SUE SFACCETTATURE

SOMMARIO

INTRODUZIONE

La sicurezza del cloud deve soddisfare i requisiti esclusivi nell'ambito di ogni singola interazione. Il **cloud pubblico** è basato su un'infrastruttura condivisa e un modello di sicurezza comune. Il **cloud privato** richiede un approccio software-defined alla sicurezza a causa della mancanza di visibilità causata dal traffico est-ovest e dai servizi virtualizzati. Il **cloud ibrido** pone una sfida: combinare le risorse interne critiche con origini dati e connessioni esterne, che richiedono una maggiore segmentazione delle risorse sulla rete.

Le odierne soluzioni di sicurezza del cloud non possono essere progettate soltanto per prevenire gli attacchi. Devono tenere conto anche del fatto che, prima o poi, saranno soggette a qualche sorta di violazione. Inoltre, devono essere robuste, al fine di garantire la protezione di risorse e utenti.

01 LA SICUREZZA A SERVIZIO DEL PARADIGMA DEL CLOUD

La soluzione di sicurezza di Fortinet è progettata appositamente per adattarsi alla natura stessa del cloud; devono quindi offrire una risorsa dinamica in grado di mutare rapidamente per proteggere tutte le varia distribuzioni: cloud pubblico, privato e ibrido.

Scalabile: la sicurezza deve adattarsi alla scalabilità ed elasticità dei carichi di lavoro del cloud. Pertanto, una funzionalità essenziale della soluzione di sicurezza di Fortinet è rappresentata dall'automazione. Le policy di rischio e accesso sono definite in anticipo affinché quando alla rete accedono nuovi dispositivi per accogliere un numero maggiore di utenti o aumentare la larghezza di banda, i dispositivi vengono configurati automaticamente.

Unica console di gestione: policy, applicazione e automazione devono essere applicati in modo uniforme sia nelle risorse statiche che dinamiche da un'unica vista dell'approccio di sicurezza globale. Nella nostra soluzione, i carichi di lavoro o sistemi classificati con un profilo di rischio comune sono trattati in modo analogo quando accedono e escono dalla rete, indipendentemente dal fatto che provengano dal data center o dal provider.

Segmentata: la capacità di segmentare sistemi, carichi di lavoro o persino componenti specifici della rete è essenziale per gestire i rischi aziendali. Il cloud, inoltre, introduce nuove sfide in termini di conformità. Quando i dati possono attraversare e persino lasciare la rete tramite il cloud pubblico, è necessario applicare la conformità dei dati per garantire il monitoraggio e il controllo di traffico, applicazioni e tipi di dati specifici.

02 SICUREZZA DEL CLOUD PUBBLICO

Il cloud pubblico rappresenta la sfida di sicurezza di più alto profilo. Solo recentemente i dirigenti e gli utenti aziendali hanno deciso di rinunciare a controllare in prima persona la propria infrastruttura, iniziando a condividere sistemi e larghezza di banda con terzi sconosciuti.

La soluzione di sicurezza del cloud di Fortinet offre carichi di lavoro sicuri nei cloud pubblici, garantendo privacy e riservatezza e sfruttando al contempo i vantaggi della scalabilità, della misurazione e del time-to-market.

Modello di sicurezza condiviso, che offre due vantaggi principali:

- La sicurezza **“del” cloud** include tutti i data center forniti dal provider di servizi cloud, che diventano responsabili della protezione.
- La sicurezza **“nel” cloud** riguarda ciò che l’utente, in qualità di abbonato al servizio cloud, offre in termini di dati e applicazioni nel cloud, di cui diventa responsabile della protezione.

La soluzione di sicurezza del cloud di Fortinet tratta i componenti dei clienti, ad esempio dati e applicazioni, sistemi operativi, gestione di accessi e identità, crittografia e traffico di rete. Tutto ciò si aggiunge alle funzionalità di sicurezza del provider per fornire protezione completa e conforme.

Integrazione del provider: la nostra soluzione, inoltre, è progettata per garantire la solida integrazione con il framework di sicurezza del provider di servizi cloud pubblici per proteggere la potenza di elaborazione, gli archivi e la connettività di rete. Offre inoltre una dashboard comune che consente di visualizzare entrambi i lati e gestire tutti gli aspetti della sicurezza.

La soluzione di sicurezza del cloud pubblico di Fortinet include:

- Supporto di tutte le principali cinque piattaforme di cloud pubblico: AWS, Azure, Google, IBM, e Oracle
- Supporto delle principali piattaforme Software-as-a-Service, tra cui Office 365 e Salesforce.com (SaaS è un'altra forma di cloud pubblico, con lo stesso livello di importanza delle piattaforme Infrastructure-as-a-Service in termini di sicurezza).
- Supporto di architetture multi-tenancy predisposte per il cloud e di domini virtuali per la segmentazione di rete
- Coordinamento del cloud nativo per l'automazione della scalabilità automatica, l'High Availability e la segmentazione.
- Interfaccia di gestione estensibile: API per ulteriore automazione e orchestrazione del cloud

03 SICUREZZA DEL CLOUD PRIVATO

La virtualizzazione funge da blocco costitutivo per offrire tutte le forme di cloud computing, ed è un aspetto particolarmente importante per la sicurezza del cloud privato. La virtualizzazione si basa su Software-Defined Networking (SDN) e altri tipi di infrastrutture software-defined, tecnologie che consentono di creare cloud privati più agili e dinamici rispetto ai data center tradizionali.

La soluzione di Software-Defined Security è certificata dalle principali piattaforme SDN e NFV (Network Function Virtualization) e può essere distribuita in qualsiasi data center trasformato in ambiente cloud.

Software-Defined Security: con la crescita dell'SDN, le risorse di rete non sono più collegate fisicamente ad hardware dedicato. In questo caso, vengono elaborate come servizi nel data center con la capacità di funzionare tra elementi o posizioni fisiche. Analogamente, la soluzione di cloud privato di Fortinet è stata progettata appositamente per offrire "servizi" di sicurezza che possono essere configurati e sottoposti a provisioning in modo dinamico. Questo approccio evolutivo estende la sicurezza a ciascun livello concettuale dell'architettura di rete: dal piano dei dati al piano di controllo al piano di gestione.

Sicurezza incentrata sulle applicazioni: quando molte applicazioni condividono la stessa infrastruttura fisica in un cloud privato, in genere non presentano gli stessi rischi. La soluzione di sicurezza del cloud di Fortinet isola i dati e le applicazioni mentre il data center continua a consolidarsi. Con l'aumento del traffico est-ovest negli ambienti software-defined, la nostra soluzione offre micro-segmentazione per separare ulteriormente tipi specifici di traffico.

La soluzione di sicurezza del cloud privato di Fortinet include:

- Supporto delle principali piattaforme SDN, tra cui VMware NSX, Cisco ACI e OpenStack
- Ulteriore coordinamento NFV per l'inserimento e il concatenamento dei servizi negli ambienti e cloud dei service provider multi-tenant
- Il dominio virtuale e multi-tenant per la segmentazione di rete e la distribuzione delle funzioni dei servizi di sicurezza
- Interfaccia di gestione estensibile: API per l'automazione e l'orchestrazione del cloud
- Unica console di gestione integrata
- Ampio ed esclusivo portfolio e opzioni di distribuzione flessibili

04 CLOUD IBRIDO

La maggior parte delle aziende sta passando da un data center in sede a un servizio di cloud pubblico e sta pianificando una combinazione di distribuzioni basate sia su IT tradizionale che su cloud pubblico. Creare un cloud ibrido dinamico richiede la migrazione aperta e sicura di grandi volumi di dati e applicazioni, connettività da sito a sito affidabile e ampliando le topologie di rete nella WAN.

La soluzione di cloud ibrido di Fortinet offre visibilità al team di sicurezza, affinché possa contare su una panoramica completa della rete, tra cui gestione end-to-end, segmentazione e protezione delle connessioni esterne.

Unica console di gestione: con risorse diffuse sia nelle aree di autenticazione fisiche che virtuali, i professionisti della sicurezza dovrebbero passare da una dashboard all'altra per disporre di vista oppure operare senza analisi centrali per la threat intelligence. La soluzione di cloud ibrido di Fortinet offre un'unica vista integrata nell'ambito di tutti i sistemi operativi nel cloud e fornisce gestione centralizzata. In questo modo, è possibile monitorare i flussi di dati nell'ambito dell'intera rete in un formato che rende tali informazioni pertinenti e fruibili.

Segmentazione: la soluzione di sicurezza del cloud ibrido di Fortinet identifica le unità di business e le applicazioni critiche non direttamente associate agli ambienti ibridi e le segmenta per ridurre al minimo l'impatto in caso di violazione. Offre inoltre la possibilità di ispezionare il traffico persistente tra i segmenti del cloud per garantire protezione da perdita dei dati e che i dati vengano smistati in base al rischio o alla policy impostata.

Connettività sicura: migrazione dei dati nelle varia posizioni, caricamento di vasti set di dati da origini esterne e sfruttamento dei servizi di analisi basati su cloud di terzi-tutto ciò richiede connessioni discrete a reti esterne. La nostra soluzione offre la giusta protezione in base al profilo di rischio di queste connessioni di rete univoche. Offre inoltre funzionalità VPN avanzate, tra cui la possibilità di fornire accesso temporaneo sicuro alle risorse quando necessario, proteggendo al contempo il resto della rete.

La soluzione di sicurezza del cloud ibrido di Fortinet include:

- Scalabilità automatica dell'efficienza della sicurezza di rete e pianificazione delle capacità
- Gestione centralizzata per il provisioning automatico
- Connettività VPN da sito a sito
- Segmentazione di connessioni persistenti
- Visibilità e controllo grazie a registri di sicurezza completi per una migliore governance di conformità

CONCLUSIONI

Fortinet è l'unica società a offrire soluzioni di sicurezza per rete, endpoint, applicazioni, data center, cloud e accesso progettate per la collaborazione con una security fabric e fornisce protezione end-to-end reale.

La nostra soluzione di sicurezza progettata ad hoc è compatibile con i principali prodotti di Fortinet per vari modelli di distribuzione del cloud, offrendo al contempo gestione centralizzata, integrazioni di API aperte, misurazione dei consumi, coordinamento delle piattaforme cloud e automazione.

Fortinet Security Fabric condivide la threat intelligence in modo dinamico con il resto dell'infrastruttura di sicurezza interconnessa. In questo modo, si riduce la necessità di più punti di contatto e policy ridondanti nelle sedi del cloud e garantisce governance sul perimetro di sicurezza a più livelli.

www.fortinet.com