SCHEDA TECNICA

McAfee VIrtual Network Security Platform

Rilevamento completo delle minacce per reti cloud

McAfee® Virtual Network Security Platform è una soluzione completa per la prevenzione delle intrusioni e delle minacce di rete (IPS) creata per le richieste specifiche di cloud pubblici e privati. Individua e blocca le minacce sofisticate nelle architetture cloud in modo semplice e preciso, consentendo alle aziende di ripristinare la conformità e adottare la protezione cloud con fiducia. Le tecnologie avanzate includono il rilevamento senza firme, l'emulazione in-line, l'applicazione di patch per le vulnerabilità basata su firma nonché il supporto per Amazon Web Services e la virtualizzazione delle reti. Con flussi di lavoro ottimizzati, molteplici opzioni di integrazione e un programma di licensing semplificato, le aziende possono gestire e scalare con facilità la sicurezza all'interno delle più complesse architetture cloud.

Protezione completa del cloud pubblico con una tecnologia di sicurezza avanzata

I cloud pubblici sono comodi, economici e offrono l'opportunità di passare da un approccio di spesa per l'infrastruttura verso un modello di spese operative. Introducono però un nuovo livello di rischio, dove una vulnerabilità in un software accessibile pubblicamente potrebbe consentire ad un aggressore di bucare il cloud ed esfiltrare informazioni riservate oppure rendere visibili involontariamente i dati di un cliente ad altri che utilizzano lo stesso servizio. McAfee Virtual Network Security Platform supporta AWS - il servizio cloud oggi più diffuso - fornendo una visibilità completa delle minacce per i dati che transitano attraverso un gateway internet nonché del traffico server to server. Grazie alla soluzione, è possibile ripristinare la visibilità sulle minacce e la conformità di sicurezza sulle architetture cloud pubbliche con una piattaforma IPS per la prevenzione delle intrusioni che offre un reale controllo del traffico server to server.

Protezione degli ambienti virtuali

Le aziende stanno velocemente adottando le infrastrutture IT virtualizzate - come cloud pubblici e privati - dove i server fisici possono ospitare contemporaneamente molteplici macchine virtuali (VM) e anche interi carichi di lavoro virtualizzati.

Vantaggi principali

Prevenzione avanzata e senza confronti contro le minacce

- Analisi malware avanzata, senza firme
- Protezione da scripting cross-site e iniezione di codice SQL
- Rilevamento avanzato callback botnet e malware
- Analisi basata sul comportamento e protezione DDoS
- Integrazione con McAfee Advanced Threat Defense
- Distribuzione IPS e sistema di rilevamento delle intrusioni (IDS)
- Soluzione sempre attiva VMware ESX-McAfee Virtual Network Security Platform

Architettura pronta per il cloud

- Una licenza permette la condivisione del throughput attraverso qualsiasi combinazione di cloud pubblico e privato.

La comunicazione tra VM risultante, unitamente a migrazione, replicazione e backup istantanei di tali carichi di lavoro, ha incrementato in modo significativo il traffico server to server all'interno di cloud pubblici e privati e SDDC. Ad aumentare il caos, la flessibilità offerta dalla virtualizzazione di rete rende il flusso di questo traffico crescente dinamico e imprevedibile. Per stare al passo, le soluzioni di sicurezza virtualizzate devono essere flessibili e scalabili e, ancor più importante, devono funzionare in modo ottimizzato con piattaforme di networking software-defined (SDN) chencontrollano questi carichi di lavoro e VM spesso di breve durata.

Stimolare l'agilità all'interno dei cloud privati

Progettata per soddisfare le richieste di protezione degli ambienti virtuali, McAfee Virtual Network Security Platform si integra perfettamente con piattaforme diffuse di cloud privato tra cui VMware NSX e ambienti SDN basati su OpenStack. Di fatto, McAfee Virtual Network Security Platform è l'unica soluzione IPS virtuale dedicata certificata a operare con VMware NSX. La micro segmentazione delle VM e l'ispezione approfondita del traffico server to server avviene automaticamente negli ambienti virtualizzati, anche per carichi di lavoro con un breve ciclo di vita.

Prevenzione senza confronti contro le minacce

McAfee Virtual Network Security Platform si basa su un'architettura di ispezione di nuova generazione progettata per fornire un controllo approfondito del traffico di rete virtuale. Utilizza una combinazione di tecniche di ispezione avanzate - tra cui l'analisi completa del protocollo, la reputazione delle minacce, l'analisi del comportamento e l'analisi avanzata del malware - per rilevare e impedire gli attacchi conosciuti e quelli di tipo zero-day sulla rete.

Nessuna tecnologia di rilevamento del malware può bloccare da sola tutti gli attacchi: per questo motivo McAfee Virtual Network Security Platform include diversi motori di rilevamento con e senza firme per impedire al malware di danneggiare gli ambienti cloud. Offre numerose tecnologie di ispezione tra cui: emulazione in-line di browser, JavaScript e file Adobe, rilevamento di botnet e callback del malware, rilevamento DDoS basato sul comportamento e protezione da attacchi avanzati come lo scripting cross-site e l'iniezione di codice SQL. McAfee Virtual Network Security Platform è inoltre in grado di identificare e bloccare i file più più furtivi tramite l'interazione con McAfee Advanced Threat Defense, laddove i file vengono presentati per un'analisi più approfondita del comportamento. McAfee Advanced Threat Defense combina analisi statica approfondita del codice, analisi dinamica (sandboxing del malware) e apprendimento automatico per incrementare il rilevamento delle minacce zero-day, include quelle che utilizzano le tecniche di evasione e il ransomware.

Semplificazione con la condivisione delle licenze cloud

Oggi, molte aziende dispiegano le loro risorse e infrastrutture IT su molteplici cloud e piattaforme, che sia per supportare le applicazioni legacy, ridurre la dipendenza da un unico vendor, la ridondanza dei sistemi o per risparmiare. Il licensing delle soluzioni di sicurezza per gli ambienti virtualizzati può essere complesso e costoso, poiché molti vendor richiedono

- L'innovativo approccio all'ispezione di AWS offre una reale protezione del traffico server to server nel cloud pubblico.
- Il supporto per l'orchestrazione con VMware NSX e ambienti SDN basati su OpenStack consentono la micro segmentazione automatizzata e l'ispezione del traffico tra carichi di lavoro di cloud privato.
- Dashboard basata su VM con funzionalità di imposizione della quarantena disponibile con l'integrazione VMware.
- Una singola console di gestione centralizzata per i sensori fisici e virtuali, on premise e nel cloud.

Gestione intelligente della sicurezza

- Una singola console gestisce i sensori on premise e nel cloud.
- Correlazione e priorità intelligenti degli allarmi.
- Robuste dashboard di indagine sul malware.
- Flussi di lavoro preconfigurati per le indagini.
- Gestione scalabile e basata sul web.

Visibilità e controllo

- Identificazione delle applicazioni.
- Identificazione degli utenti.
- Identificazione dei dispositivi.
- Stato della sicurezza di tutti i computer virtuali in AWS.

l'acquisto di licenze separate tra cloud pubblici e privati e per diverse piattaforme SDN.

McAfee semplifica il licensing e riduce i costi tramite la condivisione delle licenze cloud, un nuovo concetto che permette ai clienti di condividere il throughput e la licenza di McAfee Virtual Network Security Platform su qualsiasi combinazione di piattaforme cloud pubbliche e private. La condivisione delle licenze cloud inoltre contribuisce a migliorare la sicurezza consentendo agli amministratori di fornire rapidamente la protezione del traffico server to server e la micro segmentazione dei carichi di lavoro virtuali ovunque si trovino, senza doversi districare attraverso il processo di procurement che richiede molto tempo.

Ottimizzazione di flussi di lavoro e analisi

Individua e blocca con facilità le minacce più sofisticate. McAfee Virtual Network Security Platform include analisi e integrazioni avanzate con soluzioni di sicurezza aggiuntive per creare una piattaforma realmente completa e connessa per il rilevamento e la mitigazione delle minacce di rete.

Le minacce moderne possono generare grandi volumi di allarmi, superando rapidamente la capacità di un operatore di sicurezza di assegnare loro una priorità e tracciarli. Se non si ha un quadro completo per tempo, le minacce reali possono passare inosservate. Le analisi avanzate e i flussi di lavoro operativi di McAfee Virtual Network Security Platform correlano molteplici allarmi IPS in un unico evento fruibile, aiutando gli amministratori a ottenere direttamente le informazioni rilevanti.

Gestione centralizzata con controllo in tempo reale di dati in tempo reale

Un'appliance McAfee Network Security Manager singola offre una gestione centralizzata e basata su Web ed è eccezionalmente facile da utilizzare. La console di ultima generazione e l'interfaccia utente grafica avanzata permettono un controllo immediato dei dati in tempo reale. È possibile gestire, configurare e controllare con facilità tutte le appliance McAfee Network Security Platform, virtuali o fisiche, e le appliance McAfee Network Threat Behavior Analysis sulle risorse tradizionali e di cloud pubblico e privato da un'unica console. L'intuitiva interfaccia di gestione basata su Web è in grado di gestire qualsiasi implementazione, da dispositivi singoli fino a cluster mission-critical ampiamente distribuiti. McAfee Network Security Manager può inoltre essere implementato come istanza virtuale all'interno dei server VMware ESX e in AWS.

Elevata disponibilità e disaster recovery

McAfee Network Security Manager esegue l'arbitraggio tra i controllori e stabilisce quale è attivo e quale in standby. Quando il controller attivo diventa non disponibile, il controller in standby diventa attivo. In questo modo, viene fornita un'elevata disponibilità del controller per le distribuzioni AWS, offrendo un meccanismo di failover dove un controller è sempre attivo e raggiungibile. Inoltre, un McAfee Network Security Manager in standby assicura il disaster recovery per gli ambienti AWS.

McAfee Virtual Network Security Platform fornisce elevata disponibilità con MDR (Manager Disaster Recovery), elevata disponibilità (HA) del controller e le funzioni di auto-scaling del sensore IPS virtuale. Ciò permette a McAfee Virtual Network Security Platform di funzionare senza interruzioni. La soluzione MDR fornisce un Manager secondario, che subentra quando il Manager principale non è disponibile. Nella coppia dei controller HA, uno dei controller è sempre attivo e raggiungibile in modo che non si verifichino tempi di fermo nella rete. La funzione auto-scaling per i sensori IPS virtuali crea un nuovo sensore IPS virtuale quando un'istanza del sensore non è disponibile. Questo esegue una funzione di bilanciamento del carico ogni qualvolta si verifica un incremento del traffico di rete.

Architettura di protezione unificata

Gli attacchi sofisticati non rispettano i confini dei prodotti, sfruttando qualsiasi lacuna infrastrutturale, spacialmente tra i prodotti di sicurezza. McAfee Network Security Virtual Platform è l'unica soluzione IPS ad integrarsi con molteplici prodotti di sicurezza, sfruttando i dati e i flussi di lavoro per colmare tali lacune per un maggior ritorno sull'investimento e un costo di possesso totale ridotto. Tra le ulteriori integrazioni con i prodotti di sicurezza vi sono:

- **Software McAfee ePolicy Orchestrator® (McAfee ePO™):** completa visibilità degli endpoint per tutti gli eventi e gli allarmi IPS.
- **McAfee Endpoint Intelligence Agent:** combina le prospettive di rete ed endpoint per bloccare le perdite di dati.
- **McAfee Enterprise Security Manager:** condivisione di rich data e quarantena per gli allarmi IPS.
- **McAfee Threat Intelligence Exchange:** informazioni condivise su differenti tipologie di dispositivi.
- **McAfee Global Threat Intelligence:** il servizio di reputazione più ampio e più attivo al mondo.
- **McAfee Network Threat Behavior Analysis:** visibilità estesa a tutta la rete.
- **McAfee Virtual Advanced Threat Defense**
- **McAfee Cloud Threat Detection**
- **McAfee Management for Optimized Virtual Environments (McAfee MOVE)**
- **Scanner di vulnerabilità di terze parti:** analisi di host e rischio per gli endpoint.

Funzionalità aggiuntive

Prevenzione delle minacce avanzate

- Motore di emulazione McAfee Gateway Anti-Malware.
- Codice JavaScript incorporato in file PDF (sandbox leggera).
- Motore di analisi comportamentale Adobe Flash.
- Protezione avanzata dalle tecniche di evasione.

Protezione dai callback di botnet e malware

- Rilevamento callback a flusso veloce di DNS (Domain Name Server)/DGA (Domain Generation Algorithm).
- Sinkholing DNS.
- Rilevamento euristico dei bot.
- Correlazione degli attacchi multipli.
- Database di controllo e comando.

Prevenzione avanzata delle intrusioni

- Deframmentazione IP e riassemblaggio del flusso TCP.
- Firme McAfee, open-source e definite dall'utente.
- Messa in quarantena dell'host e limitazione della velocità.
- Ispezione degli ambienti virtuali.
- Prevenzione attacchi a negazione di servizio DoS e DDoS.
- Rilevamento basato su soglie ed euristica.
- Limitazione della connessione basata su host.
- Rilevamento ad autoapprendimento, basato su profili.

McAfee Global Threat Intelligence

- Reputazione dei file.
- Reputazione degli indirizzi IP.
- Accesso limitato basato sulla geolocalizzazione.
- Controllo degli accessi basato sull'indirizzo IP.

SCHEDA TECNICA

	Sensore di Tipo 1	Sensore di Tipo 2	Sensore di Tipo 3
Piattaforma	VMware ESX 5.5/6.0/6.5 KVM/OpenStack	VMware ESX 5.5/6.0/6.5 KVM/OpenStack	VMware ESX 5.5/6.0/6.5 NSX 6.3 AWS
Modello Sensore IPS virtuale	**IPS-VM100**	**IPS-VM600**	**IPS-VM100-VSS**[1]
Tipo di distribuzione IPS virtuale	Stand-alone	Stand-alone	Distribuito
Supporto VMware NSX	No	No	Sì
Supporto AWS	No	No	Sì
Numero di core CPU logici[2]	3	4	3
Memoria richiesta[3]	4 GB	6 GB	5 GB
Specifiche sensore virtuale			
Throughput massimo[4]	Fino a 500 Mbit/s	Fino a 1 Gbit/s	Fino a 500 Mbit/s
Connessioni contemporanee	200.000	600.000	200.000
Connessioni stabilite al secondo	6.000	20.000	6.000
Flussi UDP supportati	39.168	254.208	39.168
Numero di coppie di porte di monitoraggio	2	3	1[5]
Interfacce virtuali (VIDS) per sensore	32	100	32
Profili DoS	100	300	100
Porta di gestione	Sì	Sì	Sì
Porta di risposta	Sì	Sì	No
Modalità di distribuzione	Ispezione inter-VM, ispezione physical-to-VM, ispezione physical-to-physical, ispezione su porta SPAN		Ispezione inline VMware NSX

1. Solo per uso in ambienti VMware NSX come servizio inserito.
2. I requisiti delle risorse VM potrebbero variare a seconda della release. Consultare sempre la documentazione della release specifica.
3. Ibidem
4. Misurato con pacchetti UDP da 1.518 byte in condizioni di prova ideali.
5. Rappresentazione virtuale in ingresso e in uscita. Ispezione strettamente collegata a VMware NSX a livello del kernel.

McAfee
Together is power.

Via Fantoli, 7
20138 Milano, Italy
(+39) 02 554171
www.mcafee.com/it

McAfee, il logo McAfee, ePolicy Orchestrator e McAfee ePO sono marchi registrati o marchi di McAfee, LLC o sue filiali negli Stati Uniti e in altri Paesi. Altri marchi e denominazioni potrebbero essere rivendicati come proprietà di terzi. Copyright © 2017 McAfee, LLC. 3241_0817
AGOSTO 2017