McAfee Virtual Network Security Platform

Soluzione completa per il rilevamento delle minacce e per la prevenzione delle intrusioni per le reti cloud

McAfee® Virtual Network Security Platform (McAfee® vNSP) è una soluzione completa per il rilevamento delle minacce di rete e la prevenzione delle intrusioni (IPS) creata per soddisfare le esigenze specifiche dei cloud pubblici e privati. Individua e blocca rapidamente le minacce sofisticate nelle architetture cloud in modo semplice e preciso, consentendo alle aziende di proteggere i carichi di lavoro e ripristinare la conformità con fiducia. Integra tecnologie avanzate tra cui il rilevamento senza firme, l'emulazione in-line e l'applicazione di patch alle vulnerabilità basata su firme. Il supporto di flussi di lavoro ottimizzati per l'allocazione automatica delle risorse, opzioni di integrazione flessibili e un piano di gestione delle licenze semplificato permettono alle aziende di gestire e scalare con semplicità la loro sicurezza per soddisfare le esigenze attuali e future.

Sicurezza completa del cloud pubblico

I cloud pubblici offrono diversi vantaggi: comodità, convenienza e l'opportunità di passare da un modello di spesa per l'infrastruttura a un modello di spese operative. Introducono però un nuovo livello di rischio, laddove una vulnerabilità in un software accessibile pubblicamente potrebbe consentire ad un criminale informatico di infiltrarsi nel cloud ed esfiltrare informazioni riservate oppure rendere visibili involontariamente i dati personali di un cliente ad altri utenti che utilizzano lo stesso servizio. McAfee Virtual Network Security Platform supporta Amazon Web Services (AWS), Microsoft Azure e Oracle Cloud Infrastructure (OCI), i principali servizi di cloud pubblico attuali, fornendo visibilità completa sulle minacce e protezione per i dati che passano attraverso un gateway internet o tra server (traffico laterale est-ovest).

Protezione degli ambienti virtuali

Le aziende stanno adottando velocemente infrastrutture IT virtualizzate, come cloud pubblici e privati, dove i server fisici possono ospitare contemporaneamente molteplici macchine virtuali (VM) e carichi di lavoro virtualizzati. La comunicazione tra VM risultante, unitamente a migrazione, replicazione e backup istantanei di tali carichi di lavoro, ha incrementato in modo significativo il traffico est-ovest all'interno di cloud pubblici e privati e Data center software-defined (SDDC).

Vantaggi principali

- Protezione completa per cloud privati e pubblici (AWS, Azure e OCI)
- Modalità operativa in-line dei sistemi di prevenzione delle intrusioni (IPS)/sistemi di rilevamento delle intrusioni (IDS)
- Reale protezione del traffico est-ovest
- Policy e flusso di lavoro di gestione uniformi
- Avanzate tecnologie di ispezione per la protezione da minacce note e sconosciute
- Elevata disponibilità, disaster recovery e bilanciamento dei carichi per prestazioni ottimali
- Condivisione di licenze cloud per una maggiore flessibilità tra cloud pubblici e privati
- Integrazione nel portafoglio McAfee di soluzioni di sicurezza, dal dispositivo al cloud
- Disponibile su AWS Marketplace
- Disponibile su Azure Marketplace

Seguici

A peggiorare la situazione, la flessibilità offerta dalla virtualizzazione di rete rende questi crescenti flussi di traffico dinamici e imprevedibili. 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) che orchestrano questi carichi di lavoro e VM spesso di breve durata.

Agilità nel cloud privato

McAfee Virtual Network Security Platform può essere distribuita come appliance virtuale su un server VMware ESX per proteggere le reti virtuali all'interno di un'infrastruttura di cloud privato. Disponibile come immagine OVF (Open Virtualization Format), l'appliance virtuale permette di ispezionare il traffico tra le macchine virtuali su un particolare host ESX o tra diversi host ESX e reti fisiche.

Prevenzione delle minacce avanzate

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. La piattaforma combina diverse tecnologie 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 prevenire sia attacchi noti che quelli di tipo zero-day sconosciuti 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.

Utilizza diverse tecnologie di ispezione tra cui l'emulazione in-line di browser, codice JavaScript, file Adobe, botnet, rilevamento di callback di botnet e malware, rilevamento DDoS (Distributed Denial of Service) attraverso l'analisi comportamentale 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 furtivi tramite l'integrazione con McAfee® Advanced Threat Defense, che esegue l'analisi comportamentale sui file. McAfee Advanced Threat Defense combina analisi statica approfondita del codice, analisi dinamica (sandboxing del malware) e machine learning per migliorare il rilevamento delle minacce zero-day, incluse quelle che utilizzano le tecniche di evasione e il ransomware. McAfee offre inoltre supporto nativo per le signature Snort per rilevare e proteggere dal malware.

Condivisione flessibile delle licenze cloud

Molte aziende distribuiscono le loro risorse e infrastrutture IT su molteplici cloud e piattaforme, per supportare le applicazioni legacy, ridurre la dipendenza da un unico vendor e la ridondanza dei sistemi e per risparmiare. La gestione delle licenze delle soluzioni di sicurezza per gli ambienti virtualizzati può essere complessa e costosa, poiché molti vendor richiedono l'acquisto di licenze separate per cloud pubblici e privati.

McAfee semplifica la gestione delle licenze e riduce i costi tramite la condivisione delle licenze cloud, permettendo alle organizzazioni di condividere le loro licenze di McAfee Virtual Network Security Platform su qualsiasi combinazione di piattaforme cloud pubbliche e private.

La condivisione delle licenze cloud offre flessibilità e migliora la sicurezza consentendo agli amministratori di fornire rapidamente la protezione del traffico est-ovest e la micro segmentazione dei carichi di lavoro virtuali ovunque si trovino, senza complicati servizi di licenze e processi di procurement dispendiosi in termini di tempo.

Flussi di lavoro e analisi ottimizzati

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 la risposta è troppo lenta, le minacce reali possono infiltrarsi senza essere rilevate. McAfee Virtual Network Security Platform fornisce analisi avanzate e flussi di lavoro fruibili che correlano più avvisi IPS in un unico evento fruibile, permettendo agli amministratori di identificare rapidamente le informazioni rilevanti. Inoltre, l'integrazione con altre soluzioni di sicurezza McAfee crea una piattaforma per il rilevamento e la mitigazione delle minacce di rete realmente completa e connessa.

Policy e flusso di lavoro di gestione unificati

McAfee® Network Security Manager può essere implementato come istanza virtuale su server VMware ESX e in ambienti AWS/Azure/OCI. Gli amministratori della sicurezza possono così estendere il profilo di sicurezza on premise in modo coerente ai data center ibridi, mentre i carichi di lavoro migrano verso le piattaforme cloud, e gestirli utilizzando una console di gestione e flussi di lavoro uniformi. McAfee Virtual Network Security Platform supporta AWS Identity and Access Management (IAM), permettendo agli amministratori di gestire in modo semplice e sicuro l'accesso ai servizi e alle risorse AWS in base alle autorizzazioni assegnate a utenti e gruppi specifici.

Elevata disponibilità, disaster recovery e bilanciamento dei carichi

McAfee Virtual Network Security Platform utilizza diversi modi per offrire automaticamente controllo, protezione e prestazioni in modo continuo. McAfee Network Security Manager assicura elevata disponibilità monitorando proattivamente l'ambiente. Per esempio, lancia una nuova istanza del controllore quando un controllore attivo non è più disponibile. Inoltre, un'appliance McAfee Network Security Manager in modalità stand-by può essere distribuita per il disaster recovery in ambienti AWS, Azure e OCI.

McAfee Virtual Network Security Platform offre inoltre l'elevata disponibilità richiesta dai sensori IPS. Se un sensore non è più disponibile, la funzionalità di allocazione automatica delle risorse crea automaticamente un nuovo sensore IPS virtuale per una protezione trasparente e continua. Inoltre, se il traffico di rete aumenta, il bilanciamento automatico dei carichi tra i sensori assicura l'ottimizzazione delle prestazioni, e possono essere distribuiti automaticamente sensori aggiuntivi per soddisfare le prestazioni di throughput richieste.

Sicurezza integrata

Gli attacchi sofisticati non rispettano i confini dei prodotti, e sfrutteranno rapidamente qualsiasi vulnerabilità infrastrutturale, specialmente tra i prodotti di sicurezza. McAfee Virtual Network Security Platform è l'unica soluzione IPS a integrarsi perfettamente con molteplici prodotti di sicurezza, sfruttando efficientemente dati e flussi di lavoro tra le soluzioni per una migliore sicurezza e un maggior ritorno sull'investimento. Di seguito alcuni esempi di integrazione delle soluzioni McAfee per la sicurezza:

- **McAfee® ePolicy Orchestrator® (McAfee ePO™):** visibilità completa sugli endpoint per tutti gli eventi e gli allarmi IPS
- **McAfee® Endpoint Intelligence Agent:** combina le prospettive di rete ed endpoint per prevenire le perdite di dati
- **McAfee® Enterprise Security Manager:** condivisione di rich data e quarantena per gli allarmi IPS
- **McAfee® Threat Intelligence Exchange:** apprendimento condiviso tra 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 su tutta la rete
- **McAfee® Virtual Advanced Threat Defense:** ispezione approfondita per rilevare le minacce che utilizzano tecniche di elusione
- **McAfee® Management for Optimized Virtual Environments (McAfee® MOVE):** una soluzione antivirus per gli ambienti virtuali
- **Scanner delle vulnerabilità di terze parti:** analisi di host e rischi per gli endpoint

Funzionalità aggiuntive

Prevenzione delle minacce avanzate

- Protezione avanzata contro il malware
- Ispezione nativa del traffico SSL in entrata
- Ispezione approfondita dei file Microsoft Office
- Motore di emulazione per il codice JavaScript incorporato in file PDF (sandbox leggera)
- Motore di analisi comportamentale per Adobe Flash
- Protezione avanzata contro le tecniche di evasione

Protezione dai callback di botnet e malware

- Rilevamento dei callback "fast-flux" tramite DNS/DGA
- Reindirizzamento a un server DNS sinkhole
- Rilevamento euristico dei bot
- Correlazione di attacchi multipli
- Database del processo di controllo e comando

Prevenzione avanzata delle intrusioni

- Deframmentazione IP e riassemblaggio del flusso TCP
- Firme McAfee, open-source e definite dall'utente
- Quarantena dell'host e limitazione della velocità
- Ispezione degli ambienti virtuali
- Prevenzione degli attacchi denial-of-service (DoS) e distributed denial-of-service (DDoS)
- Liste di autorizzazione e di blocco con supporto del formato STIX (Structured Threat Information eXpression)
- Rilevamento basato su limiti e euristica
- Limitazione della connessione basata su host
- Supporto nativo per le firme Snort
- Rilevamento basato sui profili, con auto-apprendimento

McAfee Global Threat Intelligence

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

SCHEDA TECNICA

	Tipo di sensore 1	Tipo di sensore 2
Piattaforma	VMware ESX	AWS Azure OCI
Modello sensore IPS virtuale	IPS-VM600	IPS-VM600-VSS
Tipo di distribuzione IPS virtuale	Autonomo	Distribuito
Supporto AWS	No	Sì
Supporto Azure	No	Sì
Supporto OCI	No	Sì
Numero di CPU logiche	4	4
Memoria richiesta	8 GB	8 GB
Archiviazione	40 GB	40 GB
Specifiche sensore virtuale		
Throughput massimo	Fino a 1 Gbit/s	Fino a 1 Gbit/s
Numero di coppie di porte di monitoraggio	3	1 (porta di monitoraggio, non una coppia di porte)
Interfacce virtuali (VIDS) per sensore	100	100
Profili DoS	300	300
Porta di gestione	Sì	Sì
Porta di risposta	No	No
Modalità di distribuzione	Ispezione tra macchine virtuali, tra macchina fisica e virtuale, da fisica a fisica, e ispezione delle porte SPAN/in-line	

Approfondisci

- Protezione delle tue reti virtuali Amazon Web Services
- Protezione delle tue reti virtuali Microsoft Azure

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

Le funzionalità e i vantaggi delle tecnologie McAfee dipendono dalla configurazione del sistema e possono richiedere la presenza di hardware o software o l'attivazione di particolari servizi. Ulteriori informazioni sono disponibili sul sito mcafee.com/it. Nessuna rete può essere completamente sicura.

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 © 2021 McAfee, LLC. 4696_0121
GENNAIO 2021