McAfee Virtual Network Security Platform

Rilevamento completo delle minacce e prevenzione delle intrusioni 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 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. Le tecnologie avanzate includono rilevamento senza firme, emulazione in-line e applicazione di patch alle vulnerabilità basato su firme. Flussi di lavoro ottimizzati, opzioni di integrazione flessibili e un piano di licensing semplificato permette alle organizzazioni di gestire e scalare con semplicità la loro sicurezza per soddisfare le esigenze attuali e future.

Sicurezza completa del cloud pubblico

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 vNSP supporta Amazon Web Services (AWS), Microsoft Azure e Oracle Cloud Infrastructure (OCI), i principali servizi di cloud pubblico, fornendo visibilità completa sulle minacce e protezione per i dati che passano attraverso un gateway internet o da server e server (traffico laterale est-ovest).

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 carichi di lavoro virtualizzati. La risultante comunicazione tra VM, 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 data center software-defined (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

Vantaggi principali

- Protezione completa per cloud privati e pubblici (AWS, Azure e OCI)
- Reale protezione del traffico laterale est-ovest
- Console di gestione centralizzata per controllo e visibilità
- Avanzate tecnologie di ispezione proteggono da minacce note e sconosciute
- Elevata disponibilità, disaster recovery e bilanciamento dei carichi per ottime prestazioni
- Condivisione delle licenze cloud per la flessibilità tra cloud pubblici e privati
- Si integra nel portafoglio di soluzioni McAfee per una sicurezza device-to-cloud
- Disponibile nel **AWS Marketplace**
- Disponibile nel **Azure Marketplace**

Seguici su

con piattaforme di networking software-defined (SDN) che controllano questi carichi di lavoro e VM spesso di breve durata.

Agilità nei cloud privati

McAfee vNSP si integra perfettamente con le più diffuse piattaforme di cloud privato, tra cui ambienti VMware NSX e OpenStack-based SDN. McAfee vNSP 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 delle minacce avanzate

McAfee vNSP 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 sconosciuti sulla rete.

Nessuna tecnologia di rilevamento del malware può bloccare da sola tutti gli attacchi: per questo motivo McAfee vNSP include diversi motori di rilevamento con e senza firme per impedire al malware di danneggiare i tuoi cloud. Utilizza numerose tecnologie di ispezione tra cui: emulazione in-line di browser, JavaScript, file Adobe, botnet, rilevamento di 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 vNSP è inoltre in grado di identificare e bloccare i file più furtivi tramite l'interazione con McAfee Advanced Threat Defense, laddove i file vengono presentati per un'analisi del comportamento. McAfee Advanced Threat Defense combina analisi statica approfondita del codice, analisi dinamica (sandboxing del malware) e **machine learning** per incrementare 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 della licenza cloud

Le organizzazioni delle aziende dispiegano le loro risorse e infrastrutture IT su molteplici cloud e piattaforme, per supportare le applicazioni legacy, ridurre la dipendenza da un unico vendor, per la ridondanza dei sistemi e per risparmiare. Il licensing delle soluzioni di sicurezza per gli ambienti virtualizzati può essere complesso e costoso, poiché molti vendor richiedono l'acquisto di licenze separate per cloud pubblici e privati e per diverse piattaforme SDN.

McAfee semplifica il licensing e riduce i costi tramite la condivisione delle licenze cloud, permettendo alle organizzazioni di condividere le licenze e il throughput di McAfee vNSP 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 server to server 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.

Ulteriori informazioni

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

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 vNSP include analisi avanzate e flussi di lavoro processabili che correlano molteplici avvisi IPS in un unico evento processabile, 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.

Gestione centralizzata per visibilità e controllo in tempo reale

Un'appliance McAfee Network Security Manager singola offre una gestione centralizzata e basata su Web per visibilità e controllo in tempo reale. L'avanzata console offre il controllo dei dati in tempo reale tramite un unico riquadro di visualizzazione. È possibile gestire, configurare e controllare con facilità tutte le appliance McAfee Virtual Network Security Platform, virtuali o fisiche, e le appliance McAfee Network Threat Behavior Analysis negli ambienti tradizionali e di cloud pubblico e privato. L'interfaccia intuitiva inoltre è scalabile per una semplice gestione di cluster mission critical distribuiti.

McAfee Network Security Manager può inoltre essere implementato come istanza virtuale all'interno dei server VMware ESX e in ambienti AWS o Azure. McAfee vNSP 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 vNSP offre automaticamente controllo, protezione e prestazioni ininterrotte tramite diversi metodi. McAfee Network Security Manager offre elevata disponibilità monitorando proattivamente l'ambiente. Se un controller attivo non è più disponibile, McAfee Network Security Manager effettuerà automaticamente il failover a un controller in stand-by per visibilità e sicurezza senza sosta. Inoltre, McAfee Network Security Manager può essere distribuito in modalità standby per il disaster recovery in ambienti AWS, Azure e OCI.

McAfee vNSP offre inoltre elevata disponibilità per i sensori IPS. Se un sensore non è più disponibile, la funzionalità auto-scaling crea automaticamente un nuovo sensore IPS virtuale per una protezione ininterrotta. Inoltre, se il traffico di rete aumenta, il bilanciamento dei carichi automatico 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 lacuna infrastrutturale, specialmente tra i prodotti di sicurezza. McAfee vNSP 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™):** 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:** offre ispezione approfondita per rilevare le minacce evasive
- **McAfee Cloud Threat Detection:** un servizio che si collega alle esistenti soluzioni di sicurezza McAfee per rilevare il malware avanzato
- **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 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
- Individuazione euristica dei bot
- Correlazione degli attacchi multipli
- Database centralizzato

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
- Controllo degli ambienti virtuali
- Prevenzione degli attacchi denial-of-service (DoS) e distributed denial-of-service (DDoS)
- Miglioramenti alle whitelist/blacklist a supporto di STIX (Structured Threat Information eXpression)
- Rilevamento basato su soglie ed euristica
- Limitazione della connessione basata su host

- Supporto nativo per le signature Snort
- Rilevamento basato su profilo, con autoapprendimento

McAfee Global Threat Intelligence

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

	Sensore di Tipo 1	Sensore di Tipo 2
Piattaforma	VMware ESX 5.5/6.0/6.5	AWS Azure OCI VMware vSphere 6.5 e NSX 6.3
Modello sensore IPS virtuale	IPS-VM600	IPS-VM600-VSS
Tipo di distribuzione IPS virtuale	Stand-alone	Distribuito
Supporto VMware NSX	No	Sì
Supporto AWS	No	Sì
Supporto Azure	No	Sì
Supporto OCI	No	Sì
Numero di CPU logiche	4	AWS 4, Azure 5
Memoria richiesta	7 GB	7 GB
Archiviazione	8 GB	8 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 VM, da macchina fisica a virtuale, da fisica a fisica, e ispezione della porta SPAN/inline	

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

McAfee
Together is power.

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