

McAfee Network Security Platform

Un approccio alla sicurezza di rete completo e intelligente

McAfee® Network Security Platform (McAfee NSP) è un sistema per la prevenzione delle intrusioni di nuova generazione (IPS) che individua e blocca le minacce malware sofisticate presenti nella rete. Utilizza tecniche avanzate di rilevamento ed emulazione, andando ben oltre la mera corrispondenza degli schemi per difendere dagli attacchi occulti con un elevato livello di accuratezza. Per soddisfare le necessità di reti con esigenze elevate, la piattaforma è in grado di scalare a oltre 40 Gbit/s con un singolo dispositivo. Il portafoglio integrato di soluzioni McAfee ottimizza le operazioni di sicurezza unendo i feed in tempo reale di McAfee Global Threat Intelligence ai dati contestuali completi riferiti a utenti, dispositivi e applicazioni per una risposta rapida e accurata agli attacchi che si sviluppano sulle reti.

Proteggiti contro la minaccia dei moderni virus occulti

La rete deve affrontare gli attacchi dei virus occulti avanzati in grado di oltrepassare i tradizionali metodi di rilevamento, lasciando applicazioni e dati vulnerabili a violazioni e interruzioni invalidanti. Purtroppo molte organizzazioni non dispongono delle risorse finanziarie e operative per implementare e gestire la combinazione di strumenti e tecnologie necessarie per creare una difesa adeguata a questi attacchi.

La soluzione McAfee NSP combina funzioni di prevenzione delle minacce intelligenti con gestione intuitiva della sicurezza per migliorare la precisione nel rilevamento e ottimizzare le operazioni di sicurezza. Nessuna tecnologia di rilevamento del malware può

bloccare da sola tutti gli attacchi: per questo motivo McAfee NSP include diversi motori di rilevamento con e senza firme per impedire al malware di danneggiare la rete. Esegue un'analisi approfondita del traffico di rete utilizzando una combinazione di tecnologie avanzate, tra cui analisi completa dei protocolli, reputazione delle minacce e analisi comportamentale per rilevare e proteggere da attacchi callback malware, Denial of Service (DoS), zero-day e altre minacce avanzate.

Sicurezza integrata

McAfee Network Security Platform si integra con McAfee Advanced Threat Defense, che combina analisi statica approfondita del codice, analisi dinamica (sandboxing del malware) e apprendimento automatico per rilevare le minacce zero-day, incluse quelle che utilizzano le tecniche

Vantaggi principali

- Rileva e blocca le minacce rapidamente per proteggere applicazioni e dati
- Soluzione scalabile ad elevate prestazioni per ambienti dinamici
- Gestione centralizzata per visibilità e controllo
- Rilevamento avanzato, che include analisi del malware senza signature
- Decrittografia SSL in ingresso e in uscita per analizzare il traffico di rete
- Elevata disponibilità e protezione tramite disaster recovery



Seguici su:



SCHEDA TECNICA

di evasione e il ransomware. McAfee NSP adotta anche la reputazione dei file di McAfee Global Threat Intelligence e si integra con i software McAfee® ePolicy Orchestrator® e McAfee Enterprise Security Manager per una correlazione in tempo reale degli eventi di rete per tutte le risorse pertinenti. La soluzione combinata integra i dettagli dei dispositivi, le informazioni degli utenti, lo stato complessivo della sicurezza degli endpoint, le valutazioni di vulnerabilità e altre informazioni dettagliate che consentono alle aziende di comprendere meglio la gravità delle minacce e i fattori di rischio per l'attività aziendale.

Prestazioni e disponibilità

McAfee Network Security Platform offre il meglio di entrambi i mondi: sicurezza e prestazioni elevate. Combina in un unico dispositivo un'architettura di analisi single-pass, basata su protocollo, con hardware di classe carrier realizzato appositamente per un'analisi del mondo reale ad oltre 40 Gbit/s. La sua architettura efficiente preserva le prestazioni indipendentemente dalle impostazioni di sicurezza, mentre altre soluzioni IPS possono subire una riduzione del throughput fino al 50% con policy che danno priorità alla sicurezza rispetto alle prestazioni.

McAfee NSP offre anche attivo-attivo e attivo-passivo con failover stateful, permettendo di soddisfare gli accordi SLA di elevata disponibilità, evitando i colli di bottiglia delle appliance con prestazioni più lente o soluzioni standalone sovraccariche.

Visibilità e controllo

Prendi decisioni informate riguardo alle applicazioni e ai protocolli presenti sulla rete dell'azienda. McAfee Network Security Platform è la prima e unica soluzione

IPS a riunire funzioni avanzate di prevenzione delle minacce e consapevolezza delle applicazioni in un unico motore decisionale sulla sicurezza. Mettiamo in relazione l'attività delle minacce con l'utilizzo delle applicazioni, inclusa la visibilità al Livello 7 di oltre 1.500 applicazioni e protocolli, consentendo di prendere decisioni informate su quali applicazioni autorizzare sulla rete.

Oltre all'identificazione delle applicazioni, McAfee NSP consente la visibilità di utenti e dispositivi. Assegna delle priorità a host e utenti a rischio e considera anche le botnet attive, tramite l'identificazione di comportamenti di rete anomali.

Gestione intelligente e scalabile della sicurezza

Ottieni il massimo dal tuo investimento in sicurezza tramite una gestione intelligente della sicurezza di rete. McAfee Network Security Manager consente una gestione scalabile e basata sul web di un numero di appliance di sicurezza di rete compreso tra due e diverse centinaia. Offre dei flussi di lavoro a divulgazione progressiva in grado di indicare agli amministratori gli avvisi pertinenti e delle dashboard di sicurezza di facile utilizzo che automatizzano gli eventi sulla base della gravità e della pertinenza degli avvisi.

Funzionalità aggiuntive

Prevenzione delle minacce avanzate

- Le funzionalità di decrittografia Secure Sockets Layer (SSL) in ingresso supportano le codifiche Diffie-Hellman (DH) ed Elliptic-Curve Diffie-Hellman (ECDH) utilizzando una soluzione condivisa basata su agent senza impatti sulle prestazioni del sensore (in attesa di brevetto, per la serie NS)

Vantaggi principali (segue)

- Disponibile anche come appliance virtuale
- Si integra nel portafoglio di soluzioni McAfee per una sicurezza device-to-cloud

SCHEDA TECNICA

- Decrittografia SSL in uscita (serie NS)
- Motore di emulazione McAfee Gateway Anti-Malware
- Codice JavaScript incorporato in file PDF
- Motore di analisi comportamentale Adobe Flash
- Protezione avanzata dalle tecniche di evasione
- Analisi della reputazione delle minacce mobili e del cloud

Protezione dai callback di botnet e malware

- Rilevamento dei callback fast flux DNS/DGA
- Sinkholing DNS
- Individuazione euristica dei bot
- Correlazione degli attacchi multipli
- Database centralizzato

Prevenzione avanzata delle intrusioni

- Deframmentazione IP e riassetto del flusso TCP
- Firme McAfee, open-source e definite dall'utente
- Supporto nativo per le signature Snort (serie NS)
- Miglioramenti alle whitelist/blacklist a supporto di STIX (Structured Threat Information eXpression) (serie NS)
- Messa in quarantena dell'host e limitazione della velocità
- Controllo degli ambienti virtuali
- Integrazione con McAfee Advanced Threat Defense
- Supporto decompressione della risposta HTTP

Prevenzione attacchi DoS e DDoS

- Rilevamento basato su limiti e euristica
- Limitazione della connessione basata su host
- Rilevamento ad autoapprendimento, basato su profili

McAfee Global Threat Intelligence

- Reputazione di file ed IP
- Reputazione di applicazione e protocollo
- Localizzazione geografica
- Whitelisting basato sulle categorie di McAfee Global Threat Intelligence

Elevata disponibilità

- Attivo-attivo e attivo-passivo con failover stateful
- Fail-open esterno (attivo)
- Fail-open interno

Supporto per il tunneling dei protocolli

- IPv6
- Tunnel V4-in-V4, V4-in-V6, V6-in-V4 e V6-in-V6
- MPLS
- GRE
- Q-in-Q doppia rete VLAN

McAfee Network Security Manager

- Gestione multi-livello (fino a 1000 sensori)
- Autenticazione utente (RADIUS e LDAP)
- Failover e fail-back automatici
- Disaster recovery dei dati critici di configurazione
- Gestione gerarchica centralizzata delle policy
- La dashboard della memoria dettaglia l'utilizzo della memoria da parte del dispositivo

Ulteriori informazioni

Per ulteriori dettagli e le opzioni di appliance fisica, consultare la [scheda tecnica di McAfee Network Security Platform](#).



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

Le caratteristiche e i benefici offerti dalle tecnologie McAfee dipendono dalla configurazione del sistema e potrebbero richiedere l'abilitazione di hardware, software o l'attivazione del servizio. Ulteriori informazioni sono disponibili sul sito www.mcafee.com/it. Nessuna rete può essere completamente sicura.

McAfee, il logo McAfee ed ePolicy Orchestrator 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 © 2018 McAfee, LLC. 3795_0418
APRILE 2018