McAfee Advanced Threat Defense per IPS di rete

Una protezione più completa contro il malware occulto.

Principali vantaggi

- Rileva, blocca e corregge automaticamente il malware avanzato e gli attacchi furtivi che si celano nel traffico di rete.
- Aggiunge alla protezione di rete una vera funzione di analisi del codice statico e di sandboxing mirato all'obiettivo senza aumentare i carichi di lavoro dell'IPS.
- Blocca le minacce in modalità plug and play, senza ritardo dovuto all'intervento umano.

Il sistema di prevenzione delle intrusioni (IPS) di rete è un pilastro delle architetture di sicurezza aziendali. Distribuiti in banda unitamente a soluzioni di sicurezza su gateway e su host, i sistemi IPS monitorano il traffico di rete e il comportamento degli endpoint con una serie di tecniche per rilevare gli attacchi e attivare risposte in difesa.

Oggi, tuttavia, un numero crescente di minacce zero-day ignote riesce a eludere le difese convenzionali. Furtivi, ben dissimulati, adattivi in modo intelligente e spesso mirati con estrema cura, questi attacchi sofisticati costituiscono una parte ridotta ma estremamente pericolosa e costosa del mutevole panorama delle minacce.

In risposta a questi attacchi, alcune organizzazioni stanno potenziando la loro infrastruttura IPS con l'analisi dinamica sotto forma di appliance di sandboxing fuori banda. La sandbox lancia i file eseguibili sospetti in un ambiente virtuale protetto e ne monitora il comportamento in fase di esecuzione per rilevarne l'eventuale intento malevolo. Spesso, però, questo apparente guadagno in precisione di rilevamento va subito sprecato a causa della scarsa integrazione e dei processi di risposta manuali.

Ad esempio, dopo il rilevamento di un nuovo attacco, la maggior parte delle appliance di sandboxing di altre marche non è in grado di fare altro che avvertire un analista della sicurezza umano. L'analista deve creare manualmente nuove regole di blocco per l'IPS e per il firewall e quindi iniziare a identificare e correggere tutti gli endpoint compromessi durante l'analisi nella sandbox fuori banda. Le soluzioni esistenti hanno anche altri limiti comuni, fra cui:

- La necessità di predisporre un'appliance di sandboxing per ciascun sensore IPS, che fa lievitare i costi.
- La dipendenza da un ambiente di esecuzione virtuale generico che può non rilevare comportamenti di attacco specifici per un determinato obiettivo.
- La dipendenza dalla sola analisi dinamica, che rende la sandbox vulnerabile a varie strategie del malware in grado di rilevare gli ambienti protetti e di ritardare l'esecuzione del comportamento rivelatore.

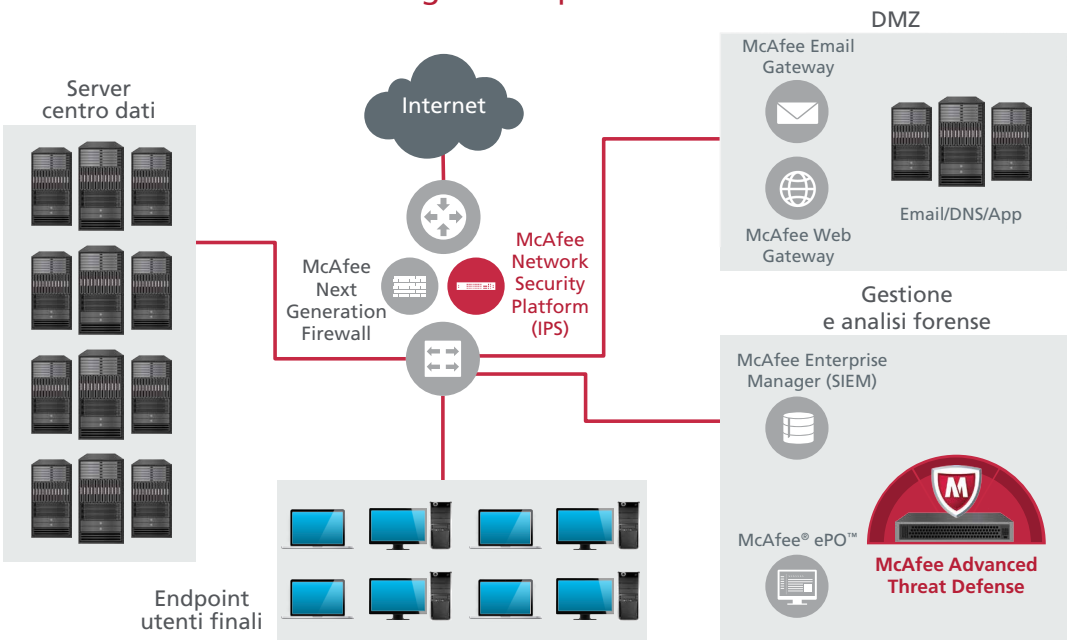
Una soluzione sandbox e IPS Security Connected

McAfee offre una soluzione a tutte queste problematiche: una perfetta integrazione fra McAfee Network Security Platform, un sensore IPS avanzato a elevate prestazioni, e McAfee Advanced Threat Defense, l'appliance di rilevamento del malware avanzato più potente e completa del settore. McAfee Network Security Platform ispeziona il traffico in banda e blocca le minacce tramite una serie di tecnologie di rilevamento del malware ottimizzate per l'esecuzione in tempo reale. McAfee Advanced Threat Defense offre una serie di analisi più completa e caratterizzata da un uso più intensivo delle risorse, che comprende sia il sandboxing mirato all'obiettivo, sia una vera e propria analisi del codice statico. Insieme, questi due dispositivi rilevano e bloccano le minacce avanzate nuove, ignote e occulte. Per una soluzione end-to-end completa, aggiungete McAfee Real Time per identificare e correggere rapidamente eventuali sistemi interessati dal malware avanzato.

- *Individuazione* — Tecnologie analitiche innovative agiscono in sinergia per rilevare rapidamente e con precisione minacce sofisticate su più protocolli.
- *Blocco* — I prodotti di sicurezza McAfee, strettamente integrati, bloccano all'istante i tentativi di infiltrazione e contengono gli endpoint infetti.
- *Correzione* — La soluzione McAfee analizza automaticamente un'infiltrazione appena rilevata in tutto l'ambiente e avvia il processo di remediation degli endpoint.

Distribuzione centralizzata

Scalabilità e costo totale di gestione più ridotto



Poiché adotta l'approccio Security Connected per l'integrazione della protezione aziendale, la soluzione McAfee Advanced Threat Defense per IPS di rete offre una serie di vantaggi operativi e di difesa unici nel settore, fra cui:

- *Blocco delle minacce plug and play* — Gli attacchi rilevati da McAfee Advanced Threat Defense vengono bloccati automaticamente da McAfee Network Security Platform senza alcun ritardo dovuto all'intervento umano.
- *Integrazione di rapporti e flussi di lavoro* — I rapporti generati da McAfee Advanced Threat Defense vengono integrati automaticamente nei flussi di lavoro di McAfee Network Security Platform, eliminando molti passaggi da uno schermo all'altro durante le indagini.
- *Visibilità degli endpoint* — McAfee Advanced Threat Defense può accedere alle informazioni di qualsiasi endpoint archiviate su McAfee Network Security Platform e sfruttarle per migliorare la precisione e la rapidità di rilevamento delle minacce.

L'IPS: McAfee Network Security Platform

McAfee Network Security Platform è una famiglia di appliance IPS (sistemi di prevenzione delle intrusioni) integrate che rileva e blocca le minacce sofisticate nella rete, compresi malware avanzato, minacce zero-day, attacchi denial-of-service e botnet. McAfee Network Security Platform abbina un'architettura di ispezione approfondita single-pass di straordinaria efficienza a componenti hardware di classe carrier realizzati appositamente. Garantisce così velocità di linea fino a 40 Gbps con un unico dispositivo, mantenendo prestazioni eccezionali in termini di throughput e di precisione indipendentemente dalle impostazioni di sicurezza. Le funzioni integrate di analisi delle minacce comprendono firme personalizzate, analisi completa dei protocolli, reputazione delle minacce, analisi approfondita dei file con emulazione e rilevamento JavaScript e correlazione fra comportamenti delle minacce e utilizzo delle applicazioni in base alla visibilità di livello 7 di oltre 1.500 applicazioni e protocolli.

Migliori insieme

- Aumentate il valore delle soluzioni di sicurezza esistenti.
- Riducete la necessità di riprogettare l'architettura di rete.
- Ampliate e automatizzate la protezione.
- Riducete al minimo remediation e indagini con un blocco in linea affidabile.
- Razionalizzate i flussi di lavoro grazie all'interfaccia di McAfee Network Security Platform.

Security Connected

La piattaforma Security Connected di McAfee costituisce una struttura unificata che consente a centinaia di prodotti, servizi e partner di imparare l'uno dall'altro, condividere dati specifici di un contesto in tempo reale e agire come un'entità unica per garantire la protezione di informazioni e di reti. Qualsiasi organizzazione può ridurre il rischio, i tempi di risposta e i costi generali e di personale grazie ai concetti innovativi, ai processi ottimizzati e ai suggerimenti pratici offerti da questa piattaforma.

Forse, la funzione più potente di McAfee Network Security Platform è la sua capacità di integrare e sfruttare le informazioni e le funzionalità di altre soluzioni di sicurezza McAfee. Per questa soluzione è di particolare importanza la perfetta integrazione con:

- Il software Real Time for McAfee® ePolicy Orchestrator® (McAfee ePO), che garantisce la visibilità in tempo reale degli endpoint e la possibilità di gestirli necessarie per isolare e correggere gli attacchi andati a buon fine.
- McAfee Enterprise Security Manager, una soluzione di gestione delle informazioni e degli eventi di sicurezza (SIEM) rivoluzionaria che offre un quadro in tempo reale dell'ambiente IT interno, abbinato e correlato al contesto globale proveniente dall'esterno. Il database perfettamente ottimizzato di McAfee Enterprise Security Manager raccoglie miliardi di eventi di registro e li correla ad altri flussi di dati pertinenti, rendendo immediatamente accessibili più anni di dati relativi agli eventi di sicurezza. Esso calcola i valori iniziali di tutti i flussi di dati in entrata per identificare le anomalie e le potenziali minacce prima che si sviluppino, e semplifica la gestione della conformità con centinaia di dashboard e rapporti relativi a obblighi specifici pronti per l'uso.
- McAfee Advanced Threat Defense, il componente per il rilevamento del malware avanzato di questa soluzione.

La sandbox: McAfee Advanced Threat Defense

McAfee Advanced Threat Defense è una soluzione di rilevamento del malware multilivello dotata di una serie flessibile di motori di ispezione e di funzioni di analisi sovrapposte che riducono progressivamente il numero dei file da esaminare via via che aumenta l'intensità di calcolo. Questo metodo esclusivo di valutazione completa ma efficiente garantisce una precisione e un'affidabilità di rilevamento elevatissime con eccellenti prestazioni in termini di throughput. Le funzioni di analisi integrate applicate da McAfee Advanced Threat Defense sono:

- Rilevamento basato sulle firme di virus, worm, spyware, bot, trojan, overflow del buffer e attacchi misti mediante una knowledge base completa creata e aggiornata da McAfee Labs, che attualmente contiene quasi 150 milioni di firme.
- Rilevamento basato sulla reputazione mediante la rete McAfee Global Threat Intelligence per rilevare le nuove minacce emergenti.
- Analisi statica ed emulazione in tempo reale per individuare rapidamente malware e minacce zero-day non identificati dalle tecniche basate su firma o reputazione.
- Analisi completa del codice statico mediante decompilazione del codice del file per valutare tutti gli attributi e i set di istruzioni e analizzare in modo approfondito il codice sorgente senza eseguirlo. Funzioni complete di decompressione sono in grado di aprire tutti i tipi di file compressi per consentire l'analisi integrale e la classificazione del malware, favorendo una migliore comprensione del tipo di malware specifico con cui si ha a che fare e dell'impatto che ha sull'azienda. L'analisi completa del codice statico fornisce informazioni essenziali sui comportamenti dipendenti dall'input e sui percorsi di esecuzione ritardati o nascosti che spesso non vengono eseguiti durante l'analisi dinamica e che le soluzioni sandbox meno ricche di funzionalità possono non rilevare.
- Analisi dinamica nella sandbox che esegue il codice del file in un ambiente di runtime virtuale e osserva il comportamento che ne risulta. Unico fra le attuali soluzioni sandbox, McAfee Advanced Threat Defense riproduce negli ambienti di runtime virtuali l'host di destinazione, ricostruito in base alle query inviate al software McAfee ePO. L'analisi del comportamento del file nelle esatte condizioni dell'host a cui era destinato consente di ottenere risultati precisi in modo rapido ed efficiente, rivelando comportamenti malevoli che potrebbero non essere attivati in un ambiente generico. Poiché molti attacchi avanzati sono studiati per eludere il rilevamento in una sandbox, McAfee Advanced Threat Defense incorpora tecniche innovative per garantire l'esecuzione del codice durante l'analisi dinamica.

Queste tecniche operano in sinergia per identificare efficacemente molti tipi di malware noto e ignoto. Combinando analisi statica e analisi dinamica complete si rivela il malware occulto e avanzato che motori di analisi meno potenti non riescono a identificare con sicurezza.

Le appliance McAfee Advanced Threat Defense sono facilmente configurabili per applicare solo le analisi non eseguite sui sensori IPS a monte, evitando di penalizzare le prestazioni con ispezioni superflue. Le capacità di throughput delle appliance McAfee Advanced Threat Defense si possono scalare fino a un massimo di 250.000 oggetti al giorno, il che permette a un solo sistema di rilevamento del malware avanzato di supportare più sensori McAfee Network Security Platform. Insieme a McAfee Network Security Platform, le appliance McAfee Advanced Threat Defense vengono gestite in modo centralizzato attraverso l'interfaccia web di McAfee Network Security Manager.

Una soluzione a ciclo chiuso efficiente per la prevenzione delle minacce avanzate

Abbinato a McAfee Network Security Platform, McAfee Advanced Threat Defense garantisce una protezione IPS di rete straordinariamente efficiente, oltre a efficacissime funzioni di rilevamento e risposta nei confronti del malware avanzato. Si tratta di una soluzione automatizzata a ciclo chiuso che individua gli attacchi sofisticati, li blocca all'istante e corregge i sistemi host interessati senza alcun intervento manuale da parte di operatori di rete o analisti della sicurezza già sovraccarichi di lavoro.

Per ulteriori informazioni su come proteggere la vostra rete dalle minacce avanzate occulte con le soluzioni McAfee, rivolgetevi al vostro rappresentante McAfee o visitate il sito www.mcafee.com/it/products/advanced-threat-defense.aspx.

McAfee Srl
via Fantoli, 7
20138 Milano
Italia
(+39) 02 554171
www.mcafee.com/it

61051brf_atd-network-ips_0514_fnl_ETMG