

McAfee Advanced Threat Defense

Rilevamento degli attacchi mirati avanzati

McAfee® Advanced Threat Defense permette alle aziende di rilevare gli attacchi mirati avanzati e di convertire le informazioni sulle minacce in azione e protezione immediate. A differenza delle sandbox tradizionali, include funzionalità di analisi aggiuntive che ampliano il rilevamento ed espongono le minacce evasive. La stretta integrazione tra le soluzioni di sicurezza - dalla rete all'endpoint - permette una condivisione immediata delle informazioni sulle minacce all'interno dell'ambiente, migliorando protezione e analisi. Opzioni flessibili per la distribuzione supportano ogni tipo di rete.

La nostra tecnologia ha trasformato l'attività di rilevamento collegando le funzioni di analisi avanzata del malware con le difese esistenti, dal perimetro della rete all'endpoint, e condividendo le informazioni sulle minacce con l'intero ambiente IT. Grazie alla condivisione delle informazioni sulle minacce fra i sistemi di gestione, rete ed endpoint, le nostre soluzioni interrompono immediatamente le comunicazioni di comando e di controllo, mettono in quarantena i sistemi compromessi, bloccano le ulteriori istanze dello stesso malware o simile, valutano se sono stati causati dei danni e agiscono.

McAfee Advanced Threat Defense: rilevamento delle minacce avanzate

McAfee Advanced Threat Defense rileva il malware zero-day furtivo odierno con un innovativo approccio

a più livelli. Combina motori di analisi statica low-touch come firme antivirus, reputazione ed emulazione in tempo reale con l'analisi dinamica (sandboxing) per analizzare il comportamento effettivo. L'indagine continua con un'analisi statica dettagliata del codice che esamina gli attributi del file e i gruppi di istruzioni per stabilire il comportamento previsto o evasivo e valuta la somiglianza con le famiglie di malware note. Come passo finale dell'analisi, McAfee Advanced Threat Defense cerca in modo specifico indicatori dannosi che sono stati identificati attraverso l'apprendimento automatico tramite una profonda rete neurale. Insieme, rappresentano la protezione più efficace disponibile sul mercato contro il malware avanzato in grado di bilanciare efficacemente le esigenze in termini di controllo approfondito e prestazioni. Mentre i metodi a minore intensità analitica, quali le

Principali elementi di differenziazione di McAfee Advanced Threat Defense

Stretta integrazione della soluzione McAfee

- Colma in tutta l'organizzazione le lacune esistenti fra scoperta, contenimento e protezione.
- Semplifica i flussi di lavoro per velocizzare risposta e remediation.

Potenti funzioni di analisi

- Utilizza una sofisticata tecnologia di decompressione per un'analisi migliore e più completa.
- Combina analisi approfondita del codice, analisi dinamica e apprendimento automatico per un rilevamento più accurato che produce dati d'analisi impareggiabili.

Distribuzione centralizzata flessibile

- Riduzione dei costi con la distribuzione centralizzata che supporta molteplici protocolli.
- Opzioni flessibili per la distribuzione supportano ogni tipo di rete.

SCHEDA TECNICA

firme e l'emulazione in tempo reale, favoriscono le prestazioni grazie all'individuazione del malware noto, aggiungendo alla sandbox l'analisi statica completa del codice e le informazioni dettagliate ottenute tramite l'apprendimento automatico si amplia la protezione contro le minacce evasive, altamente mimetizzate. Gli indicatori dannosi che potrebbero non essere eseguiti in un ambiente dinamico possono essere identificati attraverso la decompressione, l'analisi statica approfondita del codice e le informazioni dettagliate dell'apprendimento automatico.

Gli autori del malware usano la compressione per cambiare la composizione del codice o per occultarlo al fine di eludere il rilevamento. La maggior parte dei prodotti non è in grado di decomprimere correttamente l'intero codice eseguibile originale (il codice sorgente) per analizzarlo. McAfee Advanced Threat Defense include funzionalità esaurienti di unpacking che rimuovono l'offuscamento, rivelando il codice eseguibile originale. Consente l'analisi statica approfondita del codice per cercare eventuali anomalie, esaminando tutti gli attributi e i gruppi di istruzioni fino a prevedere il reale comportamento del codice stesso.

L'analisi statica approfondita del codice, l'apprendimento automatico e l'analisi dinamica, combinate insieme, offrono una valutazione completa e dettagliata del malware sospetto. Risultati d'analisi impareggiabili producono report riepilogativi che permettono un'ampia comprensione e la definizione delle priorità di azione, e report più dettagliati che forniscono dati approfonditi sul malware.

Miglioramento della protezione

Individuare il malware avanzato è importante. Se tutto ciò che una soluzione riesce a fare è generare un rapporto o segnalare un allarme, agli amministratori rimane ancora un'immensa mole di lavoro mentre la rete rimane senza protezione.

La stretta integrazione fra McAfee Advanced Threat Defense e i dispositivi di sicurezza – dal perimetro della rete all'endpoint – consente a questi ultimi di eseguire immediatamente un'azione quando McAfee Advanced Threat Defense classifica un file come dannoso. Questa stretta integrazione automatizzata fra rilevamento e protezione è fondamentale.

McAfee Advanced Threat Defense può integrarsi in modi diversi: direttamente con soluzioni di sicurezza selezionate, attraverso McAfee Threat Intelligence Exchange o McAfee Advanced Threat Defense Email Connector

L'integrazione diretta consente alle soluzioni di sicurezza McAfee di agire immediatamente sui file individuati da McAfee Advanced Threat Defense. Incorporano istantaneamente le informazioni sulle minacce nei processi esistenti di imposizione delle policy, impedendo l'ingresso nella rete delle istanze aggiuntive degli stessi file o simili.

I file malevoli individuati da McAfee Advanced Threat Defense compaiono nei registri e nelle dashboard dei prodotti integrati, come se l'intera analisi fosse stata eseguita da essi, semplificando i flussi di lavoro e consentendo agli amministratori di gestire in maniera efficiente gli allarmi tramite una singola interfaccia.

Soluzioni integrate

- McAfee Active Response
- McAfee Advanced Threat Defense Email Connector
- McAfee Enterprise Security Manager
- Software McAfee ePolicy Orchestrator®
- McAfee Network Security Platform
- McAfee Threat Intelligence Exchange
 - McAfee Application Control
 - McAfee Endpoint Protection
 - McAfee Security for Email Servers
 - McAfee Server Security
- McAfee Web Gateway

SCHEDA TECNICA

L'integrazione con McAfee Threat Intelligence Exchange amplia le capacità di McAfee Advanced Threat Defense aggiungendo ulteriori difese, come McAfee Endpoint Protection. Abilita inoltre una vasta gamma di soluzioni di sicurezza integrate per accedere ai risultati delle analisi e agli indicatori di compromissione. Se un file viene giudicato dannoso da McAfee Advanced Threat Defense, McAfee Threat Intelligence Exchange ne pubblica immediatamente le informazioni, inviando un aggiornamento della reputazione a tutte le contromisure integrate nell'organizzazione.

Gli endpoint abilitati da McAfee Threat Intelligence Exchange riescono a bloccare le primissime installazioni del malware, permettendo quindi una protezione tempestiva nel caso in cui il file ricompaia in seguito. I gateway abilitati da McAfee Threat Intelligence Exchange impediscono al file di penetrare nell'azienda. Anche se scollegati dalla rete, gli endpoint abilitati da McAfee Threat Intelligence Exchange continuano a ricevere gli aggiornamenti sui file riconosciuti come malevoli, eliminando i punti ciechi dalla consegna fuori banda dei payload.

McAfee Advanced Threat Defense Email Connector permette a McAfee Advanced Threat Defense di ricevere gli allegati email ai fini dell'analisi da un gateway di posta. McAfee Advanced Threat Defense analizza i file negli allegati e restituisce una risposta al gateway di posta che li ha inoltrati all'interno dell'instestazione del messaggio. Il gateway di posta può quindi agire in base alle policy, cancellando o mettendo in quarantena l'allegato, evitando così che il malware infetti e si diffonda sulla rete

interna. Per un rilevamento avanzato a livello di server di posta, McAfee Advanced Threat Defense si integra con McAfee Security for Email Servers attraverso McAfee Threat Intelligence Exchange.

Rilevamento e correzione dei sistemi compromessi

Per porre rimedio ad un attacco, le aziende hanno bisogno di visibilità completa, con informazioni fruibili e ordinate per priorità, al fine di prendere decisioni migliori e reagire nel modo appropriato. Le soluzioni McAfee operano di concerto per fornire alle aziende esattamente ciò di cui hanno bisogno.

McAfee Enterprise Security Manager utilizza e correla la dettagliata reputazione dei file con gli eventi di esecuzione provenienti da McAfee Advanced Threat Defense e da altri sistemi di sicurezza. Si ottengono così delle visualizzazioni avanzate degli allarmi e della cronologia che potenziano le informazioni di sicurezza, l'ordinamento dei rischi per priorità e la consapevolezza della situazione in tempo reale. Con dati relativi agli indicatori di compromissione provenienti da McAfee Advanced Threat Defense, McAfee Enterprise Security Manager tornerà indietro fino a sei mesi alla ricerca di indicazioni di tali reperti in qualsiasi dato di rete o sistema abbia conservato. Può svelare sistemi che hanno precedentemente comunicato con fonti di malware identificate di recente. McAfee Enterprise Security Manager fornisce una chiara comprensione dei rischi, in modo da intraprendere immediatamente le azioni correttive, interattive oppure automatizzate.

SCHEDA TECNICA

La stretta integrazione con McAfee Endpoint Protection, McAfee Threat Intelligence Exchange e McAfee Active Response ottimizza la risposta e l'efficienza delle operazioni di sicurezza con visibilità e interventi di mitigazione proattiva dei rischi come la creazione di nuove configurazioni, l'implementazione di nuove policy, la rimozione di file e la distribuzione degli aggiornamenti software. Interviene sulla base delle informazioni disponibili quando gli endpoint infetti sulla rete vengono identificati da McAfee Active Response ed elencati nei report di McAfee Advanced Threat Defense.

Distribuzione

Opzioni flessibili per l'analisi avanzata delle minacce supportano ogni tipo di rete. McAfee Advanced Threat Defense è disponibile come appliance in locale o virtuale. In qualsiasi versione opera come risorsa condivisa tra molteplici soluzioni McAfee, scalando in modo conveniente e riducendo i costi.

I centri operativi di sicurezza e gli analisti del malware possono inoltre usare McAfee Advanced Threat Defense per attività di indagine.

McAfee Advanced Threat Defense offre numerose funzionalità avanzate, tra cui:

- Supporto configurabile per il sistema operativo e le applicazioni: personalizza le immagini di analisi con variabili ambientali selezionate per convalidare le minacce e sostenere l'attività di indagine.

- Modalità utente interattiva: permette agli analisti di interagire direttamente con gli esempi di malware.
- Funzioni estese di decompressione: riducono il tempo di analisi da giorni a minuti.
- Percorso logico completo: permette un'analisi più approfondita degli esempi forzando l'esecuzione di percorsi logici aggiuntivi che rimangono dormienti all'interno di tipici ambienti sandbox.
- Consegna dell'esempio a molteplici ambienti virtuali: velocizza l'analisi stabilendo quali variabili ambientali sono necessarie per l'esecuzione del file.
- Report dettagliati da output disassemblati e dump della memoria a grafici delle chiamate funzionali e file incorporati o rilasciati, log utente delle API e informazioni PCAP: tale funzione offre informazioni critiche per le attività di approfondimento degli analisti.

Per ulteriori informazioni o per iniziare un periodo di valutazione di McAfee Advanced Threat Defense, contatta il tuo rappresentante o visita il sito mcafee.com/it/products/advanced-threat-defense.aspx.

SCHEDA TECNICA

Specifiche tecniche di McAfee Advanced Threat Defense

Fattore forma fisico	ATD-3100 1U montabile a rack	ATD-6100 1U montabile a rack
Fattore forma virtuale	v1008, v1016, v3032, v6064 ESXi 5.5, 6.0	v1008, v1016, v3032, v6064 ESXi 5.5, 6.0

Rilevamento

Tipi di esempi di file supportati	File PE, file Adobe, file Microsoft Office Suite, file immagine, file compressi, Java, Android Application Package, URL
Metodi di analisi	McAfee Anti-Malware Engine, reputazione GTI (file/URL/IP), Gateway Anti-Malware (emulazione e analisi comportamentale), analisi dinamica (sandboxing), analisi approfondita del codice, regole YARA personalizzate, apprendimento automatico: rete neurale profonda
Sistemi operativi supportati	Windows 10 (64 bit), Windows 8.1 (64 bit), Windows 8 (32 bit/64 bit), Windows 7 (32 bit/64 bit), Windows XP (32 bit/64 bit), Windows Server 2012, Windows Server 2012 R2, Windows Server 2008, Windows Server 2003, Android Il supporto per tutti i sistemi operativi Windows è disponibile in tutte le lingue.
Formati output	STIX, OpenIOC, XML, JSON, HTML, PDF, testo
Metodi di presentazione	Integrazioni di prodotti specifici non integrati, API RESTful, invio manuale e McAfee Advanced Threat Defense Email Connector (SMTP)



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. 3516_0817
AGOSTO 2017