McAfee Advanced Threat Defense

Rilevamento degli attacchi mirati avanzati

McAfee® Advanced Threat Defense - parte dell'offerta di prodotto di Intel Security® - 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 Intel Security - dalla rete all'endpoint - permette una condivisione immediata delle informazioni sulle minacce all'interno dell'ambiente, migliorando protezione e analisi.

Principali elementi di differenziazione di McAfee Advanced Threat Defense

Stretta integrazione con la soluzione Intel Security

- 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.
- La combinazione di analisi statica avanzata del codice e analisi dinamica permette un rilevamento più accurato che produce dati senza pari.

Analisi centralizzata del malware

- Riduce in modo efficiente, tramite l'analisi condivisa, il numero di dispositivi richiesti nella rete.
- Distribuzione semplificata.

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 similare, 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. Riunisce firme antivirus low-touch, reputazione e protezioni di emulazione in tempo reale con analisi approfondita del codice statico e analisi dinamica (sandboxing) per analizzare il comportamento effettivo. Insieme, rappresentano la protezione più efficace disponibile sul mercato contro il malware avanzato in grado di bilanciare efficacemente le esigenze in termini di protezione e prestazioni.

Mentre i metodi a minore intensità analitica, quali le firme e l'emulazione in tempo reale, favoriscono le prestazioni grazie all'individuazione del malware noto, aggiungendo alla sandbox l'analisi completa del codice statico si amplia la protezione contro le minacce evasive, altamente camuffate. Fornisce informazioni dettagliate sulla classificazione del malware tra cui la valutazione sulla somiglianza con famiglie di malware note che sfruttano il riutilizzo di codice. Le tecniche di evasione della sandbox, come i percorsi di esecuzione posticipata o contingente, spesso non eseguiti in un ambiente dinamico, possono essere rilevati tramite la decompressione e l'analisi completa del codice statico.

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 del codice statico per cercare eventuali anomalie, esaminando tutti gli attributi e i gruppi di istruzioni fino a prevedere il reale comportamento del codice stesso.

intel Security

Soluzioni integrate

- **McAfee Active Response**
- **McAfee Application Control**
- **McAfee Enterprise Security Manager**
- **McAfee ePolicy Orchestrator**
- **McAfee Network Security Platform**
- **McAfee Threat Intelligence Exchange**
- **McAfee Web Gateway**

L'analisi statica del codice e l'analisi dinamica, combinati insieme, offrono una valutazione completa e dettagliata del sospetto malware.

La sandbox specifica per il bersaglio della minaccia aumenta l'accuratezza del rilevamento
Gli attacchi mirati alla ricerca di variabili ambientali o applicazioni personalizzate possono spesso evitare il rilevamento della sandbox. Per evitarlo, McAfee Advanced Threat Defense supporta immagini personalizzate per l'analisi. Ogni azienda stabilisce non solo quali sistemi operativi ed applicazioni sono più adatti al proprio ambiente, ma anche quali versioni. Ciò consente alle aziende di analizzare le minacce nelle condizioni dell'effettivo profilo dell'host, piuttosto che di un'immagine generica, e di fornire una valutazione dei rischi più accurata.

Dato che un'azienda può avere numerosi profili host operanti nella stessa rete, McAfee Advanced Threat Defense interroga il software McAfee ePolicy Orchestrator® (McAfee ePO™) per determinare i sistemi operativi e l'elenco delle applicazioni degli host. Quindi analizza i file sospetti nelle condizioni dell'host bersaglio.

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 due modi: direttamente con soluzioni di sicurezza selezionate oppure tramite McAfee Threat Intelligence Exchange.

L'integrazione diretta consente alle soluzioni di sicurezza Intel Security 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.

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.

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. 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

McAfee Advanced Threat Defense è un'appliance per l'analisi centralizzata del malware che si inserisce perfettamente in un investimento esistente in soluzioni di sicurezza McAfee. McAfee Advanced Threat Defense funge da risorsa condivisa tra molteplici dispositivi di sicurezza Intel Security, scalando sulla rete in modo conveniente.

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:

- 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 a grafici delle chiamate funzionali e informazioni sui file incorporati o rilasciati: 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 **www.mcafee.com/it/products/advanced-threat-defense.aspx**.

Specifiche tecniche di McAfee Advanced Threat Defense	**ATD-3000**	**ATD-6000**
Fattore di forma	1U montabile a rack	2U montabile a rack
Rilevamento	**ATD-3000/ATD-6000**	
Tipi di file/media supportati	File PE, file Adobe, file Microsoft Office Suite, file immagine, file compressi, Java, Android Application Package	
Metodi di analisi	McAfee Anti-Malware Engine, reputazione GTI: file/URL/IP, Gateway Anti-Malware (emulazione e analisi comportamentale), analisi dinamica (sandboxing), analisi di codice statico, regole YARA personalizzate	
Sistemi operativi supportati	Windows 8 (32 bit / 64 bit), Windows 7 (32 bit / 64 bit), Windows XP (32 bit / 64 bit), Windows Server 2003, Windows Server 2008 (64 bit); Android Il supporto per tutti i sistemi operativi Windows è disponibile in: inglese, tedesco, italiano, giapponese e cinese semplificato.	

McAfee. Part of Intel Security.
Via Fantoli, 7
20138 Milano
Italia
(+39) 02 554171
www.intelsecurity.com