SCHEDA TECNICA DELLA FAMIGLIA

Famiglia di prodotti McAfee Endpoint Threat Defense and Response

Rileva il malware zero-day, metti in sicurezza il paziente zero e combatti gli attacchi avanzati

La sempre maggiore sofisticazione delle cyber minacce richiede una protezione di nuova generazione per gli endpoint. Le minacce avanzate e il rischio in aumento, posto dalle vulnerabilità sconosciute, stanno inducendo le aziende a individuare le soluzioni di sicurezza disconnesse e in sovrapposizione, che danno visibilità limitata e maggiore complessità. McAfee risolve questo problema con McAfee® Endpoint Threat Defense e McAfee Endpoint Threat Defense and Response. Entrambe le soluzioni si avvalgono dell'analisi statica e comportamentale e della sintesi delle informazioni per proteggere, rilevare, correggere e adattarsi al fine di combattere le minacce emergenti. I componenti di sicurezza unificati agiscono come uno solo tramite un metodo aperto e integrato, che condivide la visibilità e le informazioni sulle minacce e semplifica i flussi di lavoro. La sicurezza connessa e le analisi forensi di utilizzo pratico costituiscono un'infrastruttura protetta che identifica rapidamente e con certezza le minacce per tenere testa ai potenziali aggressori.

Sconfiggi il malware zero-day, il greyware e il ransomware

Tieni testa alle minacce emergenti con l'analisi statica e dinamica che utilizza dati potenziati su reputazioni e comportamenti per rilevare i potenziali exploit. Applica informazioni sintetizzate tramite McAfee Threat Intelligence Exchange per bloccare e contenere immediatamente le minacce e per aggiornare istantaneamente le reputazioni al fine di prevenire futuri attacchi.

Vantaggi principali

- Rileva, protegge e corregge mentre adatta proattivamente le tue difese contro il malware zero-day, il greyware e il ransomware.
- Protegge più efficacemente grazie alle reputazioni dinamiche, all'analisi comportamentale e all'apprendimento automatico.
- Riduce al minimo l'impatto sugli utenti e sulle applicazioni aziendali affidabili, grazie alla protezione rinforzata.
- Risponde e neutralizza un maggior numero di minacce e più velocemente, grazie alla condivisione delle informazioni nell'ecosistema di sicurezza.
- Semplifica l'indagine e la correzione degli eventi con i flussi di lavoro unificati e la singola console di gestione del software McAfee® ePolicy Orchestrator® (McAfee ePO™).

McAfee Endpoint Threat Defense e McAfee Endpoint Threat Defense and Response sconfiggono il malware zero-day identificando le analogie fra i comportamenti ostili esibiti e fra gli ampi modelli di minaccia di Real Protect, tramite ricerche nel cloud (centri dati situati negli Stati Uniti). Questa tecnica di classificazione dei comportamenti viene utilizzata per sradicare le minacce attive che potrebbero aver eluso le altre difese del software di sicurezza. Le informazioni di pratico utilizzo fornite tramite il software McAfee ePolicy Orchestrator consentono la scoperta fin dal giorno zero e la remediation in tempo reale. La classificazione comportamentale si evolve automaticamente tramite l'apprendimento automatico dinamico, offrendo massima protezione ed efficienza e limitando l'esposizione.

Riduci il numero degli eventi e risolvi le minacce più velocemente

Con un minor numero di eventi di sicurezza puoi concentrarti su ciò che conta di più, individuando automaticamente un maggior numero di minacce, condividendo le informazioni e utilizzando gli avvisi proattivi per definire le risposte automatiche. Allevia l'impegno necessario per indagare e neutralizzare le minacce grazie a flussi di lavoro semplificati che risolvono gli eventi più velocemente e ampliano le capacità di sicurezza, rinforzando al contempo la protezione nell'intera organizzazione.

I componenti connessi condividono automaticamente le preziose informazioni di sicurezza tramite McAfee Data Exchange Layer. McAfee Threat Intelligence Exchange ti consente di sintetizzare delle informazioni esaustive sulle minacce nell'intero ecosistema, sia da McAfee Global Threat Intelligence che da fonti di terze parti, per poi condividerle immediatamente al fine di adattare automaticamente la protezione.

Metti in sicurezza il paziente zero

Rileva e impedisci al malware zero-day di apportare modifiche dannose ai sistemi endpoint. Il contenimento dinamico delle applicazioni osserva il comportamento del greyware e previene le modifiche nocive per fermare efficacemente gli exploit ancor prima che abbiano inizio. Metti in sicurezza gli endpoint sia fuori sia dentro la rete e argina i comportamenti ostili con una protezione che è invisibile agli utenti.

Rendi scalabili e adattabili le procedure di sicurezza

L'imposizione delle policy, l'indagine dei casi e la remediation vengono semplificati tramite il software McAfee ePO: una console di gestione con un singolo pannello di controllo che dà visibilità su tutti i sistemi, così puoi valutare la condizione di sicurezza degli endpoint e attivare la protezione in tempo reale. Grazie ai flussi di lavoro unificati e alla remediation con un solo clic puoi ridurre le attività di monitoraggio, ricerca e risposta in un singolo endpoint come nell'intera infrastruttura. Con McAfee Endpoint Threat Defense e McAfee Endpoint Threat Defense and Response puoi sfruttare l'apprendimento automatico per aggiornare i modelli di classificazione dei comportamenti e condividere istantaneamente le informazioni sulle minacce fra tutti i componenti di sicurezza, in modo che possano agire come un unico sistema unificato contro le minacce emergenti. Previeni gli attacchi futuri e utilizza le risposte preconfigurate per contenere le potenziali minacce, così puoi liberare il personale e consentirgli di concentrarsi su altre priorità di gestione della sicurezza.

Scopri gli attacchi avanzati, ordinali per priorità e neutralizzali

McAfee Endpoint Threat Defense and Response ti aiuta a determinare l'origine, l'ambito e l'impatto di un attacco. Con la tecnologia McAfee Active Response hai visibilità sia attuale sia storica sugli endpoint nell'infrastruttura. Gli indicatori di attacco vengono identificati e ordinati per priorità con il contesto dettagliato, per consentire una risposta più rapida.

Vai a caccia tempestivamente e con precisione, velocità e agilità per sconfiggere le minacce che si stanno propagando attivamente, che sono in attesa o che hanno cancellato le proprie tracce per eludere il rilevamento. La visibilità e il controllo guidati dalle conoscenze permettono di capire i punti in cui le minacce stanno tentando di infiltrarsi. Il personale di intervento può immediatamente contenere e neutralizzare le minacce, riducendo l'esposizione da mesi a pochi minuti o addirittura millisecondi.

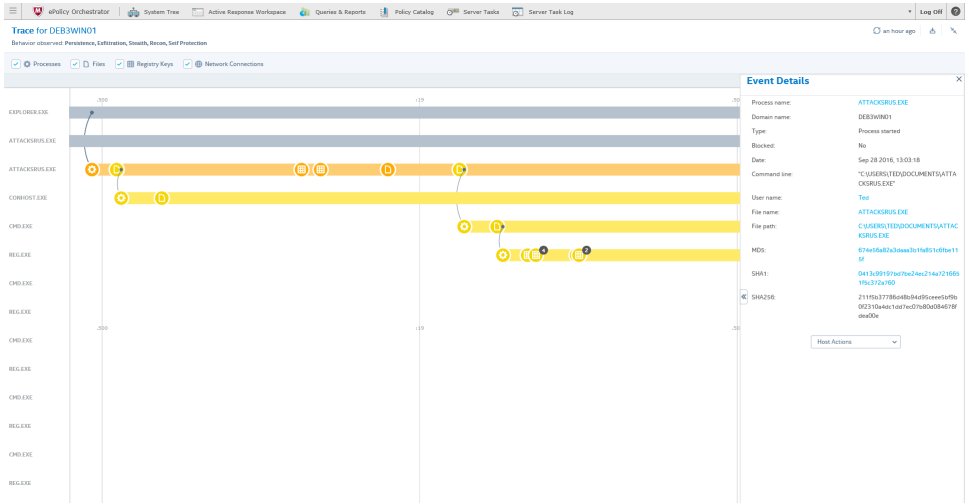

Figura 1. L'area di lavoro contro le minacce rintraccia l'origine e il comportamento degli eventi sospetti per velocizzare la risposta.

Capacità della famiglia di prodotti McAfee Endpoint Threat Defense and Response

Componente	Vantaggio	Benefici per il cliente	Differenziazione	McAfee Endpoint Threat Defense	McAfee Endpoint Threat Defense and Response
Contenimento dinamico delle applicazioni[1]	Mette in sicurezza il paziente zero impedendo al greyware di apportare modifiche nocive agli endpoint, sia dentro sia fuori la rete.	▪ Permette l'analisi delle minacce potenziali senza sacrificare il paziente zero. ▪ Rinforza la protezione senza impattare sugli utenti o sulle applicazioni affidabili. ▪ Accorcia le tempistiche dall'individuazione al contenimento con un minimo intervento manuale. ▪ Mette in sicurezza il paziente zero, mantiene la produttività degli endpoint ed esclude la rete dall'infezione.	▪ Parte integrante dell'infrastruttura McAfee per protezione ed efficienza ottimali. ▪ Funziona con o senza connessione a Internet e non richiede analisi o comandi esterni. ▪ Trasparente per l'utente. ▪ La modalità di osservazione offre una visibilità istantanea sui potenziali comportamenti di exploit nell'ambiente.	√	√
Real Protect	Applica la classificazione comportamentale dell'apprendimento automatico per bloccare il malware zero-day prima che vada in esecuzione e fermare le minacce in corso che hanno in precedenza eluso il rilevamento.	▪ Sconfigge facilmente il malware zero-day, compresi gli oggetti difficili da rilevare come il ransomware. ▪ Smaschera, analizza e neutralizza automaticamente le minacce senza la necessità di interventi manuali. ▪ Adatta le difese usando la classificazione automatica e l'infrastruttura di sicurezza connessa.	▪ L'analisi comportamentale, statica e dinamica, offre una protezione migliore rispetto ai metodi a fase singola. ▪ Rileva quel malware che può essere individuato solo tramite l'analisi comportamentale dinamica. ▪ L'integrazione approfondita condivide in tempo reale gli aggiornamenti della reputazione e aumenta l'efficacia di tutti i componenti della protezione.	√	√

SCHEDA TECNICA DELLA FAMIGLIA

Componente	Vantaggio	Benefici per il cliente	Differenziazione	McAfee Endpoint Threat Defense	McAfee Endpoint Threat Defense and Response
McAfee Threat Intelligence Exchange	Connette i componenti della sicurezza per condividere le informazioni contestuali e fornire visibilità a livello dell'intera organizzazione e il controllo per una protezione adattiva contro le minacce.	▪ Permette l'identificazione della minaccia nel paziente zero e la condivisione istantanea nel sistema di sicurezza al fine di prevenire la successiva infezione. ▪ Riduce il costo totale di proprietà e rende operativa in modo efficiente la protezione degli endpoint. ▪ Connette i componenti della sicurezza per creare una protezione a circuito chiuso tramite la trasformazione di tecnologie di sicurezza indipendenti in un singolo sistema coordinato.	▪ Sintetizza i feed provenienti da McAfee Global Threat Intelligence, da terze parti e dalle informazioni locali. ▪ Definisce cosa è affidabile e cosa non lo è tramite le informazioni locali o di terze parti. ▪ Mette istantaneamente in connessione le informazioni sulla reputazione delle minacce fra i vari prodotti endpoint, web, rete e cloud. ▪ Genera report dettagliati e fruibili con informazioni sulle minacce per adattare le difese.	√	√
McAfee Data Exchange Layer	Connette la sicurezza per integrare e semplificare le comunicazioni, sia con i prodotti di McAfee sia con quelli di terze parti.	▪ Riduce i rischi e i tempi di risposta. ▪ Riduce i carichi e i costi dovuti al personale operativo. ▪ Ottimizza i processi e dà raccomandazioni pratiche.	▪ Condivide le informazioni sulle minacce fra tutti i prodotti di sicurezza. ▪ Comunica istantaneamente a tutti gli altri endpoint l'avvenuta infezione del paziente zero, per prevenire la diffusione e aggiornare la protezione.	√	√
Piattaforma di gestione McAfee ePO	Un singolo pannello di controllo per la gestione altamente scalabile, flessibile e automatizzata delle policy di sicurezza, al fine di identificare e rispondere alle problematiche della sicurezza.	▪ Unifica e semplifica i flussi di lavoro della sicurezza per maggiore efficienza. ▪ Visibilità da un singolo pannello su tutti i sistemi per valutare subito e in tempo reale la condizione di sicurezza e la protezione. ▪ Distribuisce rapidamente e gestisce la protezione di McAfee con l'imposizione delle policy personalizzabili. ▪ Abbrevia le tempistiche dall'individuazione alla risposta grazie a interrogazioni, dashboard e reazioni dinamiche e automatizzate.	▪ Controllo granulare, costi più bassi e una gestione operativa della sicurezza più rapida tramite una singola console. ▪ Le dashboard drang and drop offrono una maggiore visibilità in tempo reale sull'intero ecosistema. ▪ I kit di sviluppo software (SDK) della piattaforma aperta facilitano la rapida adozione delle future innovazioni della sicurezza.	√	√
McAfee Active Response	Visibilità proattiva sulle minacce, cronologia degli eventi, ricerche attuali e storiche, rilevamento, capacità di prendere azioni immediate e di adattare la protezione.	▪ Ricerche rapide nei dati correnti e storici sulle minacce per determinare l'intera portata di un attacco, accelerare le indagini<e ridurre i tempi di risposta. ▪ Reazioni automatizzate alle minacce e protezione in tempo reale senza interventi manuali. ▪ Precedenza alle minacce ad alta priorità. ▪ Uso del monitoraggio continuo e di collettori personalizzabili per cercare approfonditamente gli indicatori di attacco che non solo sono in esecuzione o dormienti, ma che potrebbero anche essere stati cancellati.	▪ Visibilità istantanea sui tentativi di exploit sconosciuti e sui comportamenti rischiosi nell'ambiente, che non sono stati rilevati dalle tecnologie di protezione. ▪ Indagine sulla cronologia degli eventi di ogni endpoint con la ricerca integrata delle minacce, in tempo reale su tutti gli endpoint. ▪ Azioni con un singolo clic per proteggere, correggere e adattare, che riducono il numero di strumenti e passaggi a una sola operazione.		√

Specifiche

McAfee Endpoint Threat Defense	McAfee Endpoint Threat Defense and Response
Piattaforme supportate: ▪ Microsoft Windows: 7, To Go, 8, 8.1, 10, 10 November, 10 Anniversary ▪ Mac OS X versione 10.5 o successiva ▪ Linux: ultime versioni di RHEL, SUSE, CentOS, OEL, Amazon Linux e Ubuntu **Server:** ▪ Windows Server (2003 SP2 o successive, 2008 SP2 o successive, 2012), Windows Server 2016 ▪ Windows Embedded (Standard 2009, Point of Service 1.1 SP3 o successive) ▪ Citrix Xen Guest ▪ Citrix XenApp 5.0 o successive	**Piattaforme supportate:** ▪ Microsoft Windows: 7, 8, 8.1, 10, 10 Anniversary ▪ RedHat 6.5 ▪ CentOS 6.5 ▪ Windows Server 2008, 2012, 2016

1. McAfee Endpoint Threat Defense and Response include dei centri dati in hosting situati negli Stati Uniti, che vengono usati per convalidare l'autenticazione del cliente, verificare le reputazioni dei file e memorizzare i dati relativi al rilevamento e alla caccia dei file sospetti. Anche se non è indispensabile, una connessione al cloud ottimizza il contenimento dinamico delle applicazioni. Per funzionare al massimo, McAfee Active Response, il contenimento dinamico delle applicazioni e Real Protect richiedono l'accesso al cloud, il supporto attivo e sono soggetti alle Condizioni Generali del Servizio Cloud

Ulteriori informazioni

Maggiori informazioni sui vantaggi di McAfee Endpoint Threat Defense sono disponibili all'indirizzo **www.mcafee.com/it/products/endpoint-threat-defense.aspx.**

Maggiori informazioni sui vantaggi di McAfee Endpoint Threat Defense and Response sono disponibili all'indirizzo **www.mcafee.com/it/products/endpoint-threat-defense-response.aspx.**

McAfee
Together is power.

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