McAfee Complete Endpoint Threat Protection

Protezione dalle minacce avanzate per gli attacchi sofisticati

Il genere di minacce fronteggiato dalla tua azienda richiede un'elevata visibilità e strumenti che consentano di agire e assumere il controllo dell'intero ciclo di vita delle difese contro le minacce. Ciò significa armare i tuoi specialisti della sicurezza con la capacità di agire con maggior precisione e con informazioni approfondite sulle minacce avanzate. McAfee® Complete Endpoint Threat Protection fornisce difese avanzate che indagano, arginano e neutralizzano le minacce zero-day e gli attacchi sofisticati. La protezione endpoint di base integra l'apprendimento automatico e il contenimento dinamico per rilevare le minacce zero-day pressoché in tempo reale, classificarle e bloccarle prima che infettino i sistemi. I dati forensi fruibili e i report ti tengono informato e, in caso di violazione, ti aiutano a passare dalla reazione alle indagini, fino al rafforzamento delle tue difese. Dato che usa un framework ampliabile, puoi aggiungere con facilità altre difese dalle minacce avanzate, sia oggi sia in futuro, con l'evolversi delle tue esigenze e del panorama delle minacce.

Vantaggi principali

- Aiuta a tenere testa alle minacce zero-day, al ransomware e al greyware con l'apprendimento automatico e il contenimento dinamico.
- Velocizza la remediation e protegge la produttività con azioni e analisi automatizzate.
- Semplifica l'ambiente, la distribuzione e la manutenzione continua con la gestione centralizzata.

Difese automatizzate contro le minacce avanzate

Le minacce avanzate devono essere stroncate sul nascere. È per questo che McAfee Complete Endpoint Threat Protection include le tecnologie per il contenimento dinamico delle applicazioni (DAC) e Real Protect[1]. Quando vengono rilevati dei comportamenti ostili, il contenimento dinamico delle applicazioni argina automaticamente il greyware e le minacce zero-day sospette, per impedire che infettino i tuoi sistemi o abbiano un impatto sugli utenti.

Usando l'apprendimento automatico, Real Protect è in grado di indagare e classificare le minacce, salvando le informazioni raccolte in modo che le azioni future possano attivarsi automaticamente.

Progettato per ridurre la complessità.

La complessità è il nemico dell'efficienza. Ora non dovrai perdere tempo cercando di gestire numerose soluzioni singole, che hanno differenti interfacce e console di gestione. McAfee Complete Endpoint Threat Protection

viene gestito usando una sola console: il software McAfee® ePolicy Orchestrator® (McAfee ePO™). Con questo singolo pannello di controllo puoi iniziare rapidamente, velocizzare i tempi di distribuzione e ridurre i carichi della gestione continua. I clienti con molteplici sistemi operativi all'interno del loro ambiente potranno aumentare la loro produttività utilizzando policy multipiattaforma per sistemi basati su Microsoft Windows, Apple Macintosh e Linux.

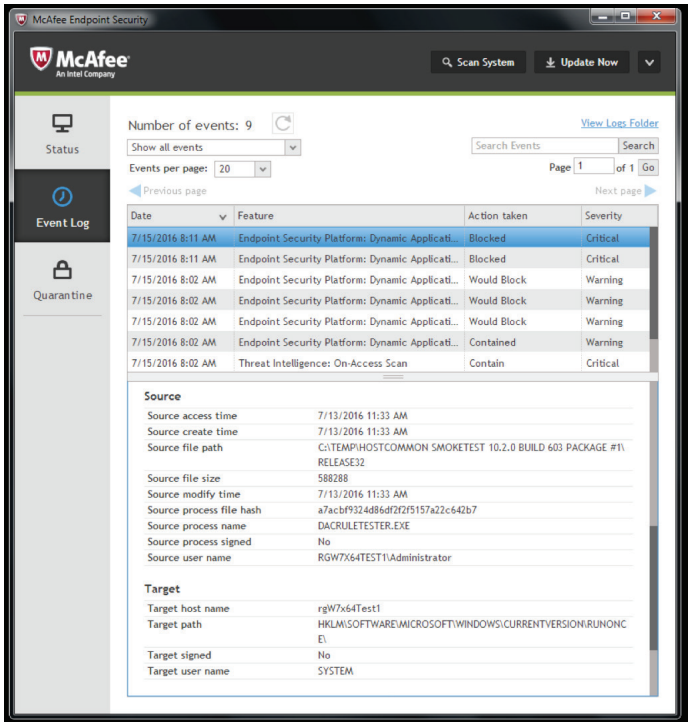

Figura 1. Il contenimento dinamico delle applicazioni blocca e argina le minacce in base alla loro gravità.

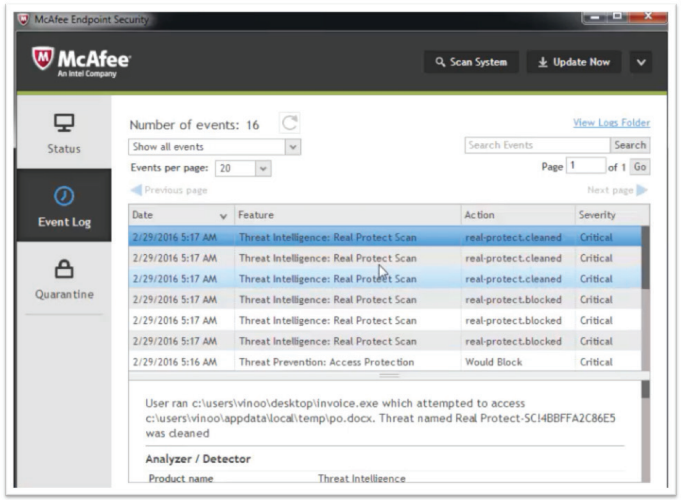

Figura 2. Real Protect utilizza l'apprendimento automatico per rilevare pressoché in tempo reale il malware che viene spesso ignorato dalle scansioni basate sulle firme.

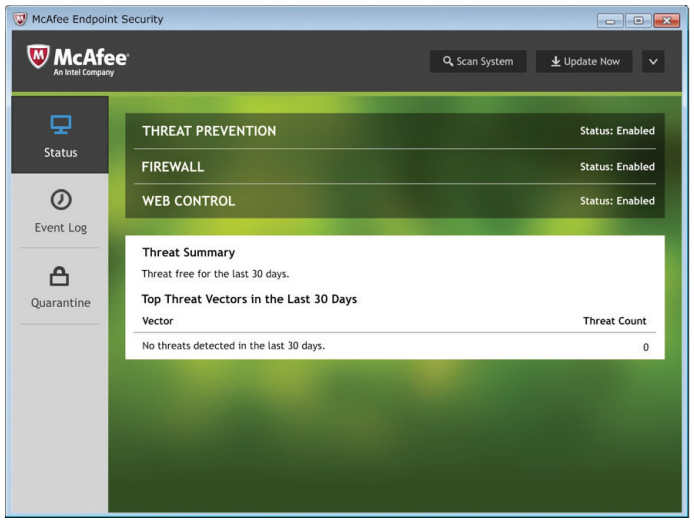

Figura 3. L'interfaccia intuitiva semplifica le attività di amministratori e utenti.

Un framework flessibile concepito per l'oggi e il domani

McAfee Complete Endpoint Threat Protection fornisce un framework connesso e collaborativo di molteplici tecnologie per una protezione pressoché in tempo reale. Ciò non consente solo un'analisi più approfondita delle minacce, ma anche la condivisione con le altre difese dei dati forensi raccolti in merito alle minacce, contribuendo a rendere le difese più intelligenti. Usando un comune livello di comunicazione, le difese di base degli endpoint possono informare e consultare quelle contro le minacce avanzate, così da avere un quadro più approfondito e stabilire la pericolosità di una minaccia non appena viene riscontrata.

Grazie a questo approccio anche la distribuzione è più flessibile, così puoi installare subito tutto ciò che è incluso con il tuo acquisto. Puoi decidere quali caratteristiche configurare e attivare ora, mentre con una variazione delle policy puoi facilmente attivare quelle che decidi di usare in seguito.

Infine, il nostro framework ti permette di espandere la protezione al variare delle tue esigenze, grazie a un'architettura progettata per includere tecnologie aggiuntive.

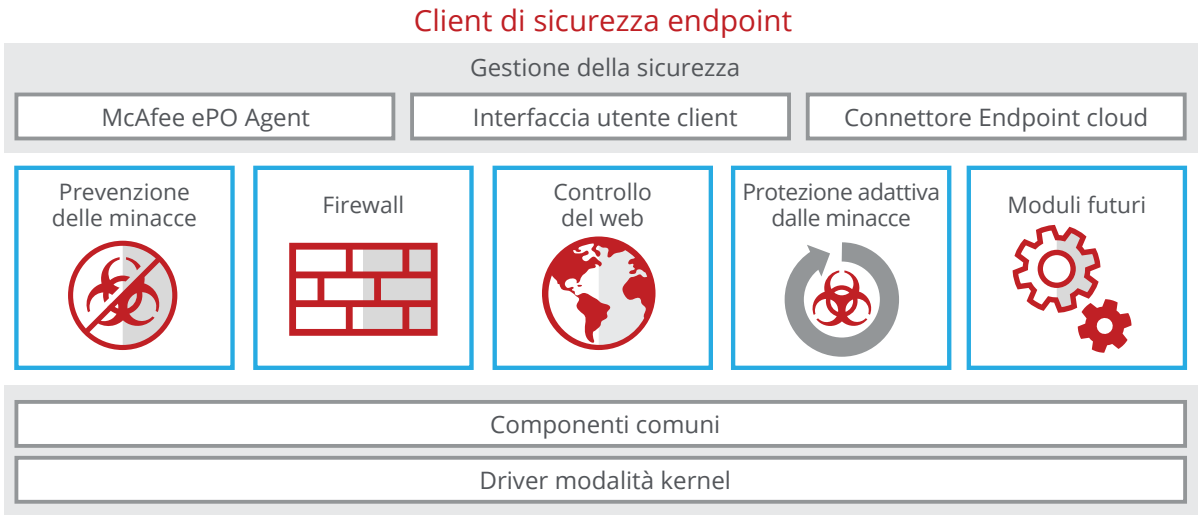

Figura 4. Il framework del client di sicurezza endpoint McAfee.

Piattaforme supportate

- Microsoft Windows: 7, To Go, 8, 8.1, 10, 10 November, 10 Anniversary
- Mac OS X versione 10.5 o successive
- Piattaforme Linux a 32 e 64 bit: 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

SCHEDA TECNICA

Componente	Vantaggio	Vantaggi per il cliente	Differenziazione
Tecnologia per il contenimento dinamico delle applicazioni	Mette in sicurezza il paziente zero impedendo al greyware di apportare modifiche nocive agli endpoint.	▪ Rinforza la protezione senza impatti sugli utenti finali o sulle applicazioni affidabili. ▪ Accorcia le tempistiche dall'individuazione al contenimento con un minimo intervento manuale. ▪ Mette in sicurezza il paziente zero ed esclude la rete dall'infezione.	▪ 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 le minacce zero-day prima che vadano in esecuzione e fermare quelle già 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.	▪ 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.
Prevenzione delle minacce	Protezione completa che trova, blocca e pone rimedio al malware grazie a molteplici livelli di sicurezza.	▪ Blocca il malware noto e sconosciuto usando tecniche euristiche e comportamentali e di scansione all'accesso. ▪ Semplifica le policy e le distribuzioni con la protezione per i computer desktop e i server Windows, Mac e Linux. ▪ Aumenta le prestazioni evitando le scansioni dei processi affidabili e dando priorità a quelli che sembrano sospetti.	Antimalware multilivello che collabora con il firewall e le difese web per rinforzare l'analisi e la prevenzione delle minacce.
Firewall integrato	Protegge gli endpoint da botnet, attacchi DDoS (Distributed Denial-of-Service), file eseguibili non attendibili, minacce avanzate persistenti e connessioni web rischiose.	▪ Protegge utenti e produttività imponendo le policy. ▪ Preserva la larghezza di banda bloccando le connessioni indesiderate in entrata e controllando le richieste in uscita. ▪ Informa gli utenti in merito a reti ed eseguibili affidabili e a file o connessioni rischiose.	Le policy relative ad applicazioni e luoghi salvaguardano i computer desktop e notebook, specialmente quando non sono nella rete aziendale.

Componente	Vantaggio	Vantaggi per il cliente	Differenziazione
Controllo del web	Assicura una navigazione sicura grazie alla protezione web e al filtraggio per gli endpoint.	▪ Riduce i rischi e tutela la conformità avvisando gli utenti prima che visitino dei siti dannosi. ▪ Previene le minacce e protegge la produttività autorizzando o bloccando l'accesso ai siti web. ▪ Blocca in maniera sicura i download pericolosi, fermandoli prima dello scaricamento.	Protezione su Windows, Mac e diversi browser.
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 attraverso l'integrazione. ▪ Riduce i carichi e i costi dovuti al personale operativo. ▪ Processi ottimizzati e raccomandazioni pratiche.	Condivide le più importanti informazioni sulle minacce fra le difese di sicurezza.
Gestione tramite McAfee ePO	Un singolo pannello di controllo per la gestione altamente scalabile, flessibile e automatizzato delle policy di sicurezza, al fine di identificare e rispondere alle problematiche della sicurezza.	▪ Unifica e semplifica i flussi di lavoro della sicurezza per una maggiore efficienza. ▪ Visibilità e flessibilità maggiori per agire con tranquillità. ▪ Veloce da distribuire e gestire con un solo agent con l'applicazione di policy personalizzabili. ▪ Abbrevia le tempistiche dall'individuazione alla risposta grazie a dashboard e report intuitivi.	▪ Maggior controllo, costi più bassi e una gestione operativa della sicurezza più rapida, con una singola console. ▪ Interfaccia collaudata che è stata ampiamente riconosciuta dal settore come superiore. ▪ Dashboard drag-and-drop in un vasto ecosistema di sicurezza. ▪ La piattaforma aperta velocizza l'adozione delle innovazioni nella sicurezza.

Ulteriori informazioni

Maggiori informazioni sui vantaggi di McAfee Complete Endpoint Threat Protection all'indirizzo: **www.mcafee.com/it/products/complete-endpoint-threat-protection.aspx**.

1. La soluzione include dei centri dati in hosting situati negli Stati Uniti, che vengono usati per verificare le reputazioni dei file e memorizzare i dati relativi al rilevamento dei file sospetti. Anche se non è indispensabile, una connessione al cloud ottimizza il contenimento dinamico delle applicazioni. Per funzionare al massimo, il contenimento dinamico delle applicazioni e Real Protect richiedono l'accesso al cloud, il supporto attivo e sono soggette alla Condizioni Generali del Servizio Cloud.

McAfee Together is power.

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