McAfee Endpoint Security

Una sicurezza progettata ad hoc per una gestione proattiva delle minacce e controlli di sicurezza comprovati

Sicurezza degli endpoint: quali sono le tue priorità?

Nelle aziende di oggi la sicurezza può essere competenza di uno o più gruppi. Nel caso delle grandi imprese, questa funzione è spesso condivisa tra diversi gruppi, ad esempio, uno responsabile dell'amministrazione IT e l'altro delle operazioni di sicurezza. Qualunque sia l'approccio che meglio riflette il tuo ruolo nell'azienda, le tue priorità influenzano inevitabilmente le caratteristiche e i risultati che ti aspetti dalla tua piattaforma di protezione del terminale.

La soluzione per la protezione degli endpoint a cui ti affidi deve quindi essere allineata con le tue priorità. A prescindere dal ruolo che ricopri, McAfee® Endpoint Security si adatta alle tue esigenze critiche, dal blocco e monitoraggio delle minacce alla personalizzazione dei controlli di sicurezza. McAfee® MVISION Insights assegna le priorità alle minacce per consentirti di agire prima che si verifichi un attacco. La soluzione ti permette di garantire la disponibilità dei sistemi per gli utenti, identificare ulteriori opportunità di automazione e semplificare i flussi di lavoro complessi.

Disponibilità e visibilità

McAfee Endpoint Security consente ai clienti di gestire il ciclo di difesa contro le minacce e di rispondere in modo efficace con difese proattive e strumenti di correzione. La correzione tramite ripristino automatico riporta lo a stato di integrità dei sistemi per preservare la produttività di utenti e amministratori, evitando loro di dover attendere l'applicazione delle misure correttive, il ripristino a seguito di un incidente oppure la ricostruzione dell'immagine di un computer infetto. Le informazioni globali sulle minacce e quelle locali e in tempo reale sugli eventi sono condivise fra gli endpoint e la soluzione McAfee® MVISION EDR per raccogliere i dettagli degli eventi relativi alle minacce, rilevare e bloccare quelle minacce che tentano di eludere l'individuazione e correlarle al framework MITRE ATT&CK per un'analisi più approfondita. La gestione è semplice grazie a una console centralizzata che può essere distribuita in ambienti locali, virtuali o in modalità SaaS. MVISION Insights offre una visibilità e un controllo unici sulle minacce potenziali con un'elevata propensione all'attacco e determina se il livello di sicurezza di un'azienda è sufficiente a bloccare tali minacce. La soluzione garantisce un livello avanzato di protezione contro le minacce critiche e sventa gli attacchi prima che si verifichino.

Vantaggi principali

- **Difese avanzate per minacce avanzate:** apprendimento automatico, monitoraggio del furto delle credenziali e misure correttive di ripristino dello stato precedente che completano le funzionalità di sicurezza di base dei sistemi desktop e server Windows.
- **Nessuna ulteriore complessità:** gestisci le tecnologie McAfee, le policy di Windows Defender Antivirus, le impostazioni di Defender Exploit Guard e Windows Firewall utilizzando un'unica policy e un'unica console.

Seguici

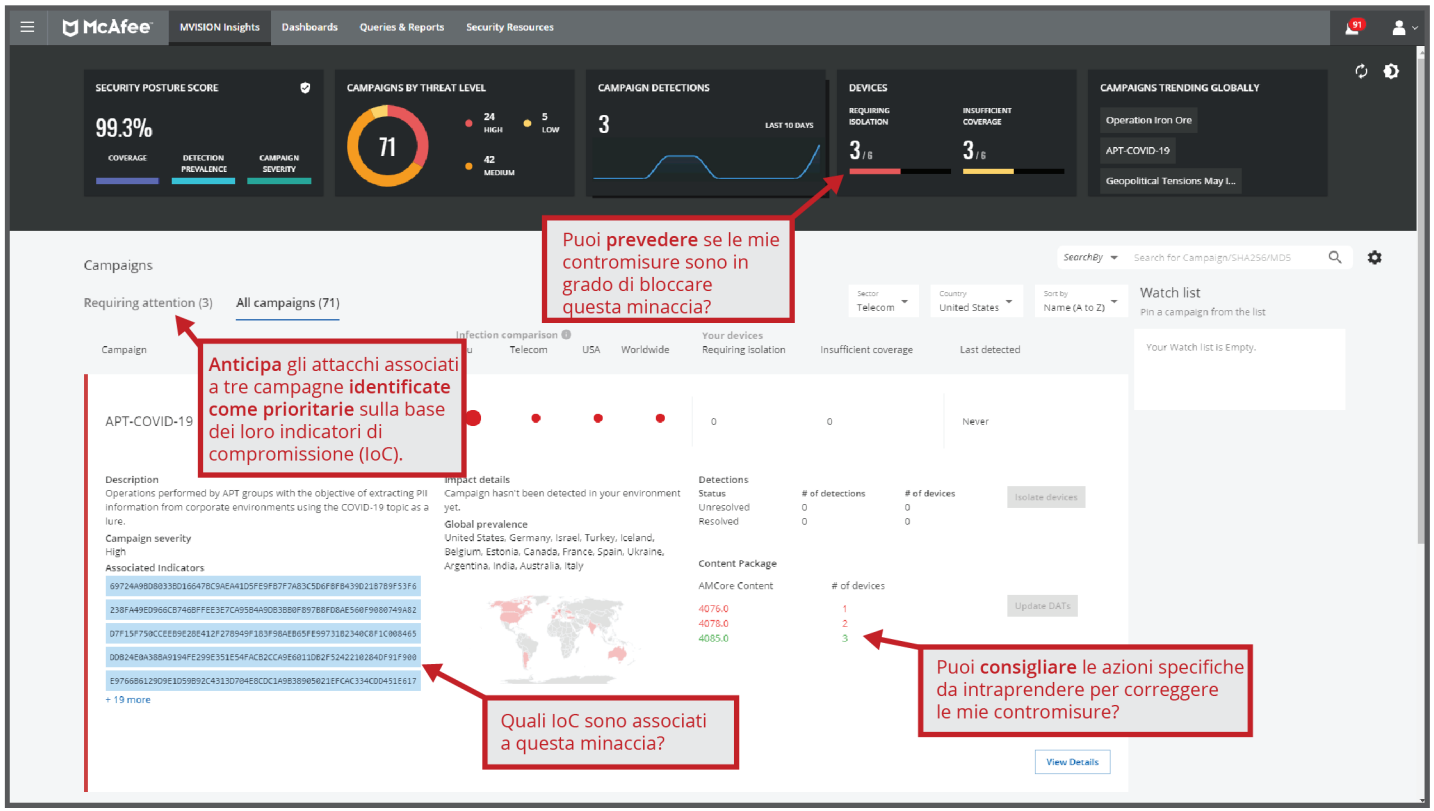

Figure 1. Dashboard di MVISION Insights. (Per funzionare correttamente MVISION Insights ha bisogno dei dati telemetrici di McAfee Endpoint Security (Opt-in).)

Grazie a MVISION Insights le aziende ricevono allarmi e notifiche sulle potenziali minacce prioritarie che potrebbero colpirli in base al settore e all'area geografica. Inoltre, MVISION Insights offre una valutazione locale del livello di sicurezza e stabilisce se è sufficiente a proteggere l'azienda da tali minacce. Identifica inoltre gli endpoint vulnerabili a minacce specifiche e offre suggerimenti prescrittivi sulle azioni da intraprendere, sostenendo gli sforzi proattivi per stare un passo avanti ai criminali informatici che potrebbero passare all'offensiva.

Vantaggi principali

- **MVISION Insights:** reagisci all'istante alle campagne d'attacco cui sei maggiormente esposto in funzione della loro attività nel tuo settore o nella tua regione geografica grazie a questa soluzione di threat intelligence all'avanguardia, che fornisce informazioni di sicurezza immediatamente fruibili. MVISION Insights identifica in anticipo i dispositivi dotati di una protezione insufficiente contro queste campagne specifiche e offre suggerimenti per migliorare il rilevamento. È l'unica soluzione per la sicurezza degli endpoint sul mercato che stabilisce in modo predittivo un piano d'azione prescrittivo e basato su priorità.

McAfee Endpoint Security raccoglie le informazioni sulle minacce provenienti da più livelli di interazione tramite un singolo agent software, eliminando così le ridondanze tipiche della concomitanza di diversi prodotti singoli. Ne risulta un approccio integrato alla sicurezza che elimina i processi manuali di correlazione delle minacce. Le informazioni sulle minacce che richiedono un'analisi ulteriore vengono trasmesse automaticamente ai team di risposta agli incidenti. I dati sulle minacce sono presentati in un formato semplice e chiaro tramite la funzione Story Graph, che visualizza informazioni dettagliate sulle minacce e consente agli amministratori di risalire alle fonti degli attacchi e di analizzarle.

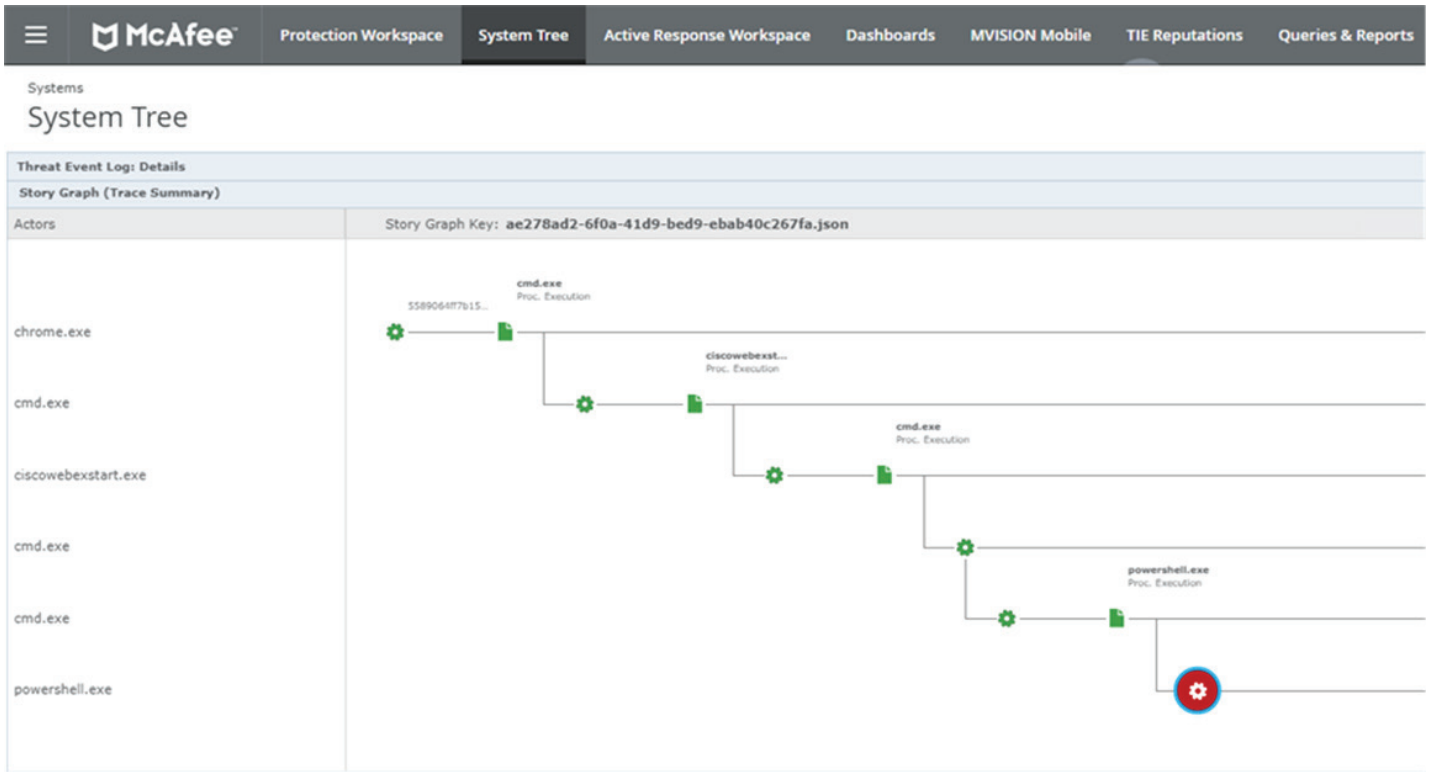

Figure 2. Story Graph.

Protezione integrata contro le minacce avanzate che automatizza gli interventi e velocizza i tempi di risposta

Inoltre, il framework integrato di McAfee Endpoint Security include funzionalità di protezione aggiuntive contro le minacce avanzate per aiutare le aziende a difendersi contro le minacce avanzate più recenti[1]. Ad esempio, la funzione di contenimento dinamico delle applicazioni analizza il greyware e altri malware emergenti e li isola per per prevenire infezioni.

Un'altra tecnologia per contrastare le minacce avanzate è Real Protect, che sfrutta la classificazione dei comportamenti tramite il machine learning per migliorare il rilevamento del malware zero-day. La classificazione priva di firme viene eseguita nel cloud, consuma poche risorse del client e assicura un rilevamento pressoché in tempo reale. Le informazioni fruibili fornite possono essere utilizzate, tra l'altro, per creare indicatori di attacco (IoA) e indicatori di compromissione (IoC). Ciò può risultare particolarmente utile per individuare gli attacchi di spostamento laterale, identificare "pazienti zero", attribuire attacchi ai criminali informatici, condurre indagini digitali e applicare misure correttive. Real Protect consente inoltre di accelerare le analisi successive ottimizzando automaticamente la classificazione dei comportamenti per identificarli e aggiungendo regole per individuare futuri attacchi simili, utilizzando funzionalità dinamiche e statiche.

Infine, per prevenire immediatamente l'infezione e ridurre i tempi di risposta degli amministratori della sicurezza IT, il client ripristina l'ultima configurazione corretta nota dell'endpoint che è stato individuato come compromesso.

Protezione intelligente degli endpoint che segnala tempestivamente cosa fanno gli aggressori informatici

Grazie alla disponibilità di migliori informazioni si possono ottenere risultati migliori. McAfee Endpoint Security condivide in tempo reale le sue osservazioni con le diverse tecnologie di difesa degli endpoint collegate alla propria infrastruttura. In questo modo possono collaborare e accelerare l'identificazione dei comportamenti sospetti, migliorare il coordinamento delle difese e rafforzare la protezione contro gli attacchi mirati e le minacce zero-day. Informazioni come il valore di hash dei file, gli URL di origine, gli eventi AMSI e PowerShell sono tracciati e condivisi non solo con altri sistemi di protezione, ma anche con le interfacce client e di gestione, per aiutare gli utenti a comprendere meglio gli attacchi e fornire agli amministratori analisi fruibili delle minacce.

Inoltre, la tecnologia McAfee® Threat Intelligence Exchange permette alle difese adattive di collaborare con altre soluzioni di McAfee, inclusi gateway, sandbox e la nostra soluzione per la gestione delle informazioni e degli eventi di sicurezza (SIEM). La raccolta e distribuzione delle informazioni di sicurezza a livello locale, globale e comunitario, riducono il tempo che intercorre tra la scoperta di un attacco e la sua neutralizzazione da diverse settimane o mesi a pochi millisecondi.

Combinato con McAfee® Global Threat Intelligence (McAfee® GTI), il framework McAfee Endpoint Security si avvale del cloud per monitorare e rispondere in tempo reale all'intero spettro delle minacce nuove ed emergenti in tutti i vettori: file, web, email e rete. Il sistema esistente di protezione e gestione degli endpoint viene ottimizzato tramite le informazioni locali e globali sulle minacce, per contrastare all'istante il malware sconosciuto e mirato. Azioni automatizzate su applicazioni e processi sospetti permettono di rispondere rapidamente alle nuove forme di attacchi emergenti, mentre le informazioni vengono inviate gli altri sistemi di difesa e alla comunità globale.

I clienti che utilizzano il contenimento dinamico delle applicazioni e Real Protect ottengono informazioni dettagliate sulle minacce più avanzate e i relativi comportamenti. Ad esempio, il contenimento dinamico delle applicazioni fornisce informazioni sulle applicazioni sottoposte a contenimento e sul tipo di accesso che tentano di procurarsi, come il registro e la memoria.

Real Protect offre informazioni sui comportamenti dannosi e classifica le minacce in modo che le aziende che cercano di raccogliere informazioni sui processi dannosi che interessano gli endpoint possano utilizzarle per rintracciare il malware e facilitare i team di risposta agli incidenti. Tali informazioni possono risultare particolarmente utili per scoprire le tecniche utilizzate dal malware basato su file per eludere il rilevamento: compressione, crittografia o abuso di applicazioni legittime.

Prestazioni elevate ed efficaci per rispondere tempestivamente

Per quanto intelligente possa essere una soluzione di sicurezza, è di scarso valore se ostacola il lavoro degli utenti con analisi lente, lunghe installazioni o una gestione complicata. McAfee Endpoint Security protegge la produttività degli utenti grazie a un livello di servizio comune e al nostro nuovo motore antimalware, che contribuiscono a ridurre le risorse e la potenza di calcolo utilizzate dal sistema di un utente. Le analisi degli endpoint non influiscono sulla produttività degli utenti perché vengono eseguite solo quando il dispositivo è inattivo e riprendono in modo trasparente dopo il riavvio o lo spegnimento del sistema.

Il processo di analisi adattiva limita inoltre le richieste alla CPU da parte di un meccanismo di apprendimento dei processi e delle fonti affidabili, al fine di concentrare le risorse solo su processi che sembrano sospetti o la cui fonte è sconosciuta. McAfee Endpoint Security integra un firewall che usa McAfee GTI per proteggere gli endpoint da botnet, attacchi di negazione di servizio distribuita (DDoS), minacce avanzate persistenti e connessioni web pericolose.

Maggior durata, minor complessità

Con la rapida proliferazione dei prodotti di sicurezza con funzionalità ridondanti e console di gestione separate è diventato molto difficile ottenere un quadro chiaro dei potenziali attacchi. McAfee Endpoint Security offre una protezione affidabile e a lungo termine, grazie alla sua struttura aperta ed espandibile, che costituisce la base per la centralizzazione delle soluzioni per gli endpoint attuali e future. Questo framework sfrutta il livello Data Exchange Layer per consentire la collaborazione con le tecnologie di altre soluzioni già disponibili, preservando gli investimenti dell'azienda in sicurezza. L'architettura integrata a sua volta si integra perfettamente con gli altri prodotti McAfee per colmare le lacune della sicurezza, ridurre i compartimenti tecnologici isolati ed eliminare le ridondanze, migliorando inoltre la produttività grazie alla riduzione dei costi operativi e della complessità di gestione.

Il software McAfee® ePolicy Orchestrator® (McAfee ePO™) semplifica ulteriormente la gestione grazie a un singolo pannello di controllo dal quale monitorare, distribuire e gestire gli endpoint. Le viste personalizzabili e i flussi di lavoro facili da comprendere e utilizzare forniscono gli strumenti per valutare rapidamente il livello di sicurezza, individuare le infezioni e mitigare l'impatto delle minacce mettendo in quarantena dei sistemi, bloccando i processi dannosi e impedendo i trafugamenti di dati. La console fornisce anche un punto centralizzato per la gestione di tutti gli endpoint, altre funzionalità McAfee e oltre 130 soluzioni di terze parti.

SCHEDA TECNICA

Funzione	Beneficio
Rilevamento e neutralizzazione delle minacce proattivi (MVISION Insights)	▪ Rileva le potenziali minacce in modo predittivo e preventivo in base al tuo settore e all'area geografica. ▪ Valuta localmente il tuo livello di sicurezza contro le potenziali minacce e le misure correttive. ▪ Contrasta i criminali informatici applicando le difese prima che si verifichi un attacco.
Real Protect	▪ La funzione di classificazione del comportamento basata sul machine learning rileva le minacce zero-day pressoché in tempo reale, fornendo informazioni fruibili sulle minacce. ▪ Ottimizza automaticamente la classificazione dei comportamenti per individuarli e aggiunge regole per rilevare attacchi futuri.
Protezione degli endpoint contro gli attacchi mirati	▪ La protezione degli endpoint riduce il tempo che intercorre tra il rilevamento e la neutralizzazione dell'attacco da giorni a pochi millisecondi. ▪ McAfee Threat Intelligence Exchange raccoglie le informazioni da svariate fonti, consentendo ai componenti della sicurezza di comunicare istantaneamente l'uno con l'altro in merito agli attacchi avanzati emergenti e multifase. ▪ La registrazione degli eventi AMSI e PowerShell rileva gli attacchi senza file e quelli basati sugli script e fornisce protezione.
Scansione intelligente e adattiva	▪ Bypassando la scansione dei processi approvati e dando la priorità ai processi e alle applicazioni sospetti prestazioni e produttività migliorano. ▪ L'analisi adattiva dei comportamenti monitora le attività, prende di mira gli eventi sospetti e trasmette gli allarmi necessari.
Ripristino delle azioni correttive	▪ Annulla automaticamente le modifiche apportate dal malware e ripristina l'ultima configurazione di sistema corretta, preservando al contempo la produttività degli utenti.
Sicurezza web proattiva	▪ La protezione proattiva per il web assicura una navigazione sicura grazie alla protezione web e al filtraggio per gli endpoint.
Contenimento dinamico delle applicazioni	▪ La soluzione DAC difende da ransomware e greyware e mette in sicurezza il "paziente zero"[2].
Blocco degli attacchi di rete	▪ Il firewall integrato usa i punteggi di reputazione basati su McAfee GTI per proteggere gli endpoint da botnet, attacchi DDoS, minacce APT e connessioni web sospette. ▪ La protezione del firewall autorizza solo il traffico in uscita durante l'avvio del sistema, per proteggere gli endpoint che non sono collegati alla rete aziendale.
Story Graph	▪ Gli amministratori possono identificare rapidamente i sistemi infetti, le cause dell'infezione e la durata dell'esposizione, al fine di comprendere la minaccia e reagire più rapidamente.
Gestione centralizzata (piattaforma McAfee ePO) con diverse opzioni di distribuzione	▪ Gestione centralizzata che offre maggiore visibilità, semplifica le operazioni, aumenta la produttività del reparto IT, unifica la protezione e riduce i costi.
Framework aperto ed estensibile per la sicurezza degli endpoint	▪ Un'architettura integrata consente ai prodotti di protezione degli endpoint di collaborare e comunicare per una difesa più robusta. ▪ In questo modo i costi operativi si riducono eliminando le ridondanze e ottimizzando i processi. ▪ La perfetta integrazione con altri prodotti di McAfee e di terze parti colma le lacune nella protezione.

Tabella 1. Caratteristiche principali e vantaggi

Un passo avanti rispetto alle minacce informatiche

McAfee Endpoint Security offre ciò di cui hanno bisogno adesso i professionisti della sicurezza per guadagnare una posizione di vantaggio rispetto ai criminali informatici: difese intelligenti e collaborative e una struttura che semplifica gli ambienti complessi. Grazie a prestazioni elevate ed efficienti e a un rilevamento delle minacce efficace, come dimostrato da test indipendenti, le aziende possono proteggere gli utenti, migliorarne la produttività e garantirne la tranquillità.

McAfee, leader di mercato nel settore della sicurezza per gli endpoint, offre una gamma completa di soluzioni di difesa approfondita e proattiva grazie alla combinazione di potenti funzioni di protezione e un sistema di gestione efficiente. Tale approccio consente ai team di sicurezza di neutralizzare le minacce in modo più rapido e con meno risorse.

Migrazione semplificata

Gli ambienti in cui sono installate le versioni correnti del software McAfee ePO, di McAfee VirusScan® Enterprise e di McAfee® Agent possono sfruttare il nostro strumento di migrazione automatica per trasferire le policy esistenti verso McAfee Endpoint Security in 20 minuti o meno[3].

McAfee Endpoint Security assicura anche i seguenti vantaggi:

- Analisi a impatto zero per una maggiore produttività degli utenti
- Dati di analisi digitale più completi relativi alla funzionalità Story Graph permettono di ottenere un quadro immediato della situazione e di semplificare le indagini per aiutarti a rafforzare le policy
- Il ripristino delle misure correttive permette di annullare automaticamente le modifiche apportate dal malware e di preservare l'integrità dei sistemi
- Informazioni proattive sulle potenziali minacce prioritarie e suggerimenti prescrittivi sull'adozione di contromisure contro le minacce con MVISION Insights
- Un minor numero di agent da gestire e di analisi superflue, per ridurre l'inserimento manuale
- Funzioni di protezione collaborative che lavorano insieme per contrastare le minacce avanzate
- Una struttura di nuova generazione che può essere integrata con altre soluzioni avanzate di rilevamento e risposta alle minacce per gli endpoint (EDR)

Ulteriori informazioni

Per saperne di più su McAfee Endpoint Security, vai qui.

Per saperne di più sul modo in cui McAfee Endpoint Security completa il portafoglio prodotti di McAfee, visita:

- MVISION Endpoint
- Famiglia di prodotti MVISION
- McAfee Threat Intelligence Exchange
- MVISION EDR
- McAfee ePolicy Orchestrator
- MVISION Insights

1. Disponibile con la maggior parte delle suite McAfee per gli endpoint. Consulta il tuo rappresentante commerciale per i dettagli.
2. Ibidem
3. I tempi di migrazione dipendono dalle policy e dall'ambiente esistenti.

McAfee

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