McAfee ePO Deep Command

La gestione della sicurezza oltre il sistema operativo riduce i costi operativi.

Riduci gli interventi di supporto alle scrivanie degli utenti e alle telefonate al supporto tecnico, dovuti a eventi di sicurezza, epidemie o password di crittografia dimenticate. Finalmente, gli amministratori della sicurezza possono distribuire, gestire e aggiornare la sicurezza sugli endpoint spenti, disattivati o crittografati. Il software McAfee® ePO™ Deep Command[1] si avvale della tecnologia Intel® vPro™ Active Management Technology (AMT) per la gestione dei sistemi automatizzata oltre il sistema operativo che permette di ridurre i costi operativi, aumentare sicurezza e conformità e accelerare la remediation in remoto dei PC e dei dispositivi a funzione fissa.

Vantaggi principali

- **Rapida rilevazione e fornitura di Intel AMT:** facile individuazione dei PC dotati di Intel vPro e attivazione di Intel AMT per un'installazione ottimizzata.
- **Sblocco in sicurezza:** quando opera con le suite McAfee Complete Data Protection, McAfee ePO Deep Command può sbloccare in modo sicuro e ottenere accesso all'ambiente di preavvio di un endpoint crittografato.
- **Riduzione dei tempi di remediation:** gestione in remoto della remediation su qualsiasi PC o endpoint ovunque nel mondo, con accesso dall'hardware.
- **Miglioramento della produttività dell'utente:** esecuzione di attività esigenti in termini di risorse durante i periodi di inattività per limitare l'impatto sugli utenti finali.
- **Riduzione dei costi dell'IT:** riduzione dei frequenti interventi di supporto alle scrivanie degli utenti e delle lunghe chiamate di servizio.
- **Riduzione dei costi del consumo elettrico degli endpoint:** adozione di programmi di risparmio energetico, mantenendo l'accesso per scopi di sicurezza o applicazione di patch.

Gli amministratori della sicurezza sono assediati da costi, minacce informatiche e requisiti aziendali in continuo aumento. Ogni intervento presso la scrivania dell'utente a causa di un'infezione malware o di altre minacce può costare fino a 250 dollari. Oltre al costo, è inoltre difficile raggiungere fisicamente la scrivania di ogni utente. Uffici remoti, telelavoratori e impiegati mobili si affidano alle chiamate al supporto tecnico e a spedizioni notturne al deposito. Essendo molto impegnati, questi utenti sono spesso ignari dei problemi e lavorano su sistemi non conformi e vulnerabili finché il malware non provoca un guasto grave, un blocco o un'interruzione.

Allo stesso tempo, il panorama delle minacce per gli endpoint pone gni giorno un maggior numero di problematiche legate alla sicurezza. I criminali informatici si muovono rapidamente per sfruttare le nuove vulnerabilità, usando botnet e siti web per propagare malware occulto e zero-day. Alcuni tipi di malware possono addirittura disattivare le contromisure poste al livello del sistema operativo, rendendo inutilizzabile il PC e di dispositivi a funzione fissa dell'utente finale.

A complicare le cose, i responsabili informatici posti sotto pressione per ridurre i consumi energetici, considerano i desktop inattivi come un elemento "ecologico". Vorrebbero spegnere i sistemi inutilizzati ma anche disporre di un modo affidabile per gestire sicurezza e conformità ed eseguire i processi informatici - scansioni, aggiornamenti o patch - nei momenti in cui tali attività influenzano meno gli utenti.

Come individuare e abilitare le tue piattaforme Intel vPro

Il software McAfee ePO Deep Command aiuta a ottenere il massimo dalla tecnologia Intel vPro, sfruttando il temporizzatore Intel AMT, le funzioni di attivazione remota e il commutatore Tastiera Video Mouse, oltre che il reindirizzamento IDE. Innanzitutto, il modulo McAfee ePO Deep Command Discovery and Reporting rileva qualsiasi PC ed endpoint abilitato AMT nell'ambiente dell'azienda. Rapporti dettagliati aiutano a individuare quali PC ed endpoint debbano ricevere l'agent McAfee ePO Deep Command. Il software McAfee ePO Deep Command ottimizza anche il provisioning di Intel AMT per semplificare l'attivazione di Intel AMT. Dopo aver installato il software McAfee ePO Deep Command sui PC ed endpoint AMT forniti, è possibile gestire da remoto questi PC oltre il sistema operativo, a livello hardware.

intel Security

Requisiti di sistema

- Software McAfee ePO 4.6 (modulo Discovery and Reporting); software McAfee ePO 4.6 (McAfee ePO Deep Command); software McAfee ePO 5.0 e versioni successive
- McAfee Agent 4.5 o versioni successive
- McAfee Drive Encryption 7.0 e versioni successive (per funzionalità di gestione della crittografia da remoto)
- Supporta i sistemi operativi Microsoft Windows XP, Windows Vista, Windows 7, Windows 8, Windows Server 2003 e Windows Embedded XP
- Supporta Intel vPro AMT versione 2.2 e successive
- Intel Setup and Configuration Software (SCS) 8.2 e versioni successive

La gestione remota come soluzione

A questo punto, gli amministratori della sicurezza possono comunicare e assumere il controllo degli endpoint a livello di hardware, che siano spenti, disattivi o crittografati. Questa connessione all'hardware permette una gestione remota per l'applicazione di policy di sicurezza o conformità, riducendo i costi operativi connessi alla sicurezza. Oltre a migliorare lo stato complessivo della sicurezza, questi controlli permettono di adottare programmi di gestione dell'alimentazione al fine di risparmiare energia, mantenendo l'accesso agli endpoint. Utilizzando la tecnologia Intel vPro AMT, il software McAfee ePO Deep Command accede agli endpoint senza doversi affidare al sistema operativo. Questo accesso a livello di hardware consente agli amministratori di attivare i sistemi, eseguire le attività legate alla sicurezza e infine riportare gli endpoint al loro stato precedente di consumo energetico. Il software McAfee ePO Deep Command è persino in grado di avviare in sicurezza il processo di avvio degli endpoint su cui è in esecuzione il software McAfee Complete Data Protection (crittografia dell'endpoint) senza che l'utente debba inserire le credenziali di autenticazione per svolgere attività di sicurezza in remoto. Tali operazioni possono tutte verificarsi automaticamente con un temporizzatore "power-on" oppure su richiesta.

Comunicando con gli endpoint a un livello posto oltre il sistema operativo, il software McAfee ePO Deep Command permette di configurare e correggere gli endpoint difficili da gestire da un sito centralizzato con la familiare piattaforma di gestione del software McAfee ePO.

Attivazione ed esecuzione

Gli amministratori possono condurre attività di manutenzione della sicurezza o attività che richiedono molto tempo, durante i periodi di inattività dei computer, così che gli utenti non vengano disturbati. Utilizzando AMT Alarm Clock, gli amministratori della sicurezza possono accendere e attivare gli endpoint, anche se crittografati, per eseguire attività di sicurezza, fra le quali, a titolo informativo:

- Aggiornamenti di configurazione e sicurezza (.DAT compresi).
- Scansioni su richiesta.
- Installazione di ulteriori prodotti di sicurezza.
- Reportistica degli eventi.
- Installazione di patch ad applicazioni o al sistema operativo.

Ripristino fuori banda degli endpoint disabilitati

Quando si verificano dei problemi, come nel caso di un sistema operativo disabilitato o di un disco rigido guasto, sia gli amministratori che gli utenti traggono vantaggio dalla comodità della gestione integrata attivata tramite il software McAfee ePO Deep Command. Che l'endpoint o il PC sia locale o remoto, l'amministratore può connettersi al Pc o endpoint disabilitato e al commutatore Tastiera Video Mouse tramite AMT per effettuare un'azione risolutiva in remoto, quale riavviare il PC da un'altra immagine .ISO presente in rete. Nella maggior parte dei casi, l'endpoint non deve essere collegato via cavo alla rete. McAfee ePO Deep Command può gestire endopoint con il Wi-Fi abilitato in modo sicuro.

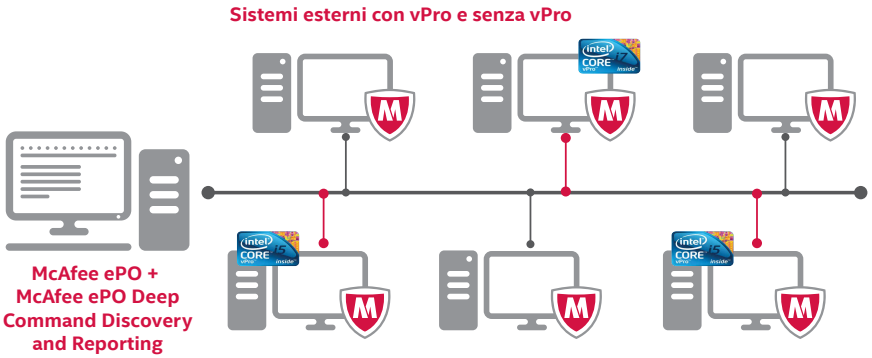

Figura 1. McAfee ePO Deep Command può individuare i sistemi vPro e distribuire il software per abilitare Intel AMT.

La funzione Intel AMT "Fast Call for Help" offre agli utenti un modo facile per contattare gli amministratori del software McAfee ePO per ricevere assistenza. L'amministratore del software McAfee ePO può rapidamente:

- Reindirizzare l'endpoint ad avviarsi da un'immagine posta su un'altra posizione in rete.
- Controllare completamente il commutatore Tastiera Video Mouse locale.
- Reimpostare la password di cifratura dell'utente.
- Pulire e riparare i sistemi infetti, disabilitati o in quarantena, senza accedervi direttamente.

Sicurezza al passo con le minacce

Con queste ampie possibilità di controllo, i team della sicurezza dispongono di nuove opzioni per giocare d'anticipo nella protezione degli endpoint contro le minacce emergenti. I sistemi possono essere aggiornati prima che una minaccia potenziale li raggiunga, mentre le contromisure sono attivabili in remoto, prevenendo gli eventuali impatti sulla produttività degli utenti e mantenendo al sicuro i dati.

Riduzione dei costi del consumo elettrico degli endpoint

Dato che il software McAfee ePO Deep Command può attivare gli endpoint, aggiornarne le policy e poi riportarli in modo sicuro allo stato di basso consumo, la tua azienda può abbracciare senza timori i programmi di risparmio energetico e accedere agli incentivi per la riduzione dei consumi, senza compromettere la sicurezza. Contatta McAfee per scoprire quale potrebbe essere il risparmio energetico per la tua azienda.

Scalabilità e reportistica a livello aziendale

Il software McAfee ePO Deep Command rafforza l'infrastruttura di gestione del software ePolicy Orchestrator® (McAfee ePO™), collaudata per estendersi a centinaia di migliaia di endpoint. Progettata per supportare le architetture distribuite e i team di gestione della sicurezza, il software McAfee ePO fornisce una gestione delle policy di sicurezza e un ambiente di reportistica unificati per l'intera infrastruttura di sicurezza McAfee. Da ora può portare "oltre il sistema operativo" anche le le policy e iniziative legate alla conformità della tua azienda. Con una maggiore quantità di informazioni da poter includere nelle dashboard e nei rapporti del software McAfee ePO, è possibile aumentare la visibilità sulla conformità di ogni endpoint, oltre che sullo stato complessivo della sicurezza dell'organizzazione. La correlazione dei dati semplifica il momento della verifica.

Ulteriori informazioni all'indirizzo **www.mcafee.com/it/products/epo deep command.aspx**.

Il software McAfee ePO Deep Command è disponibile come prodotto autonomo o all'interno delle suite McAfee Complete Data Protection. Ulteriori informazioni sono disponibili sul sito **www.mcafee.com/it/products/data-protection/index.aspx**.

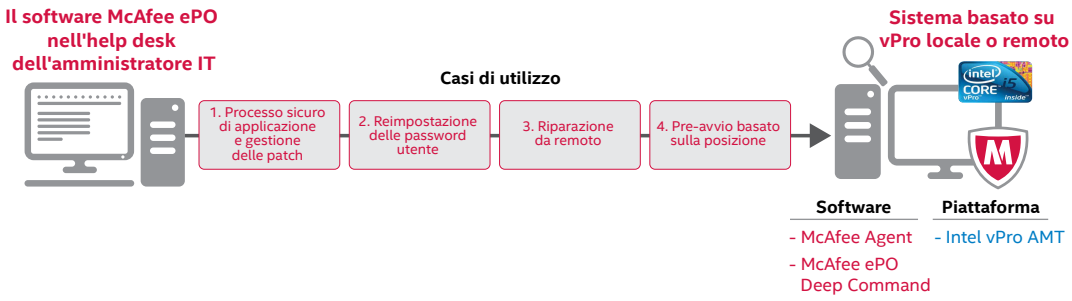

Figura 2. McAfee ePO Deep Command permette all'help desk di eseguire diversi compiti, in locale o da remoto.

1. Il software McAfee ePO Deep Command è disponibile come prodotto autonomo o all'interno delle suite McAfee Complete Data Protection. Ulteriori informazioni sono disponibili sul sito **www.mcafee.com/it/products/data-protection/index.aspx**.

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