



McAfee ePO Deep Command

**Senkung der Betriebskosten dank Sicherheitsverwaltung
jenseits des Betriebssystems**

Hauptvorteile

- **Schnelle Erkennung und Bereitstellung von Intel AMT:** Einfache Identifizierung von Computern mit Intel vPro und anschließende Aktivierung von Intel AMT
- **Sicheres Entsperren:** In Kombination mit den McAfee Complete Data Protection-Suites kann McAfee ePO Deep Command verschlüsselte Endgeräte sicher entsperren und auf die Pre-Boot-Umgebung zugreifen
- **Schnellere Problembhebung:** Verwaltung der Problembhebung per Fernzugriff auf beliebigen PCs oder Endgeräten überall auf der Welt durch Zugriff auf die Hardware

Mit der neuen Lösung von McAfee lassen sich Support-Besuche am Arbeitsplatz, Helpdesk-Telefonate durch Sicherheitsvorfälle, Virenausbrüche oder vergessene Verschlüsselungskennwörter einschränken. Jetzt können Sicherheitsadministratoren ausgeschaltete, defekte oder verschlüsselte Endgeräte neu aufsetzen, verwalten und deren Sicherheit auf den neuesten Stand bringen. Die Software McAfee® ePO™ Deep Command¹ nutzt die Intel® vPro™ Active Management Technology (AMT) zur automatisierten Sicherheitsverwaltung über das Betriebssystem hinaus. Die Technologie ermöglicht die Senkung der Betriebskosten, die Optimierung der Sicherheit und Compliance sowie die schnellere Problembhebung bei Remote-PCs.

Sicherheitsadministratoren kämpfen mit steigenden Kosten, zunehmenden Bedrohungen und wachsenden Geschäftsanforderungen. Jeder durch Malware oder andere Bedrohungen verursachte Support-Besuch am Arbeitsplatz kann Kosten in Höhe von bis zu 250 US-Dollar verursachen. Mitunter ist es auch schwierig, persönlich am Arbeitsplatz jedes Benutzers zu erscheinen. Externe Geschäftsstellen, Telearbeiter sowie mobile Mitarbeiter müssen sich auf Service-Desk-Anrufe und Expresszustellungen an das Service-Depot verlassen können. Diese vielbeschäftigten Nutzer ignorieren Probleme häufig und arbeiten mit nicht konformen, gefährdeten Systemen, bis es aufgrund von Malware zu einem katastrophalen Fehler, einer Gerätesperrung oder einer Unterbrechung kommt.

Gleichzeitig werden die Sicherheitsbedrohungen für Endgeräte von Tag zu Tag gefährlicher. Internetkriminelle passen ihre Methoden schnell an, um neue Schwachstellen auszunutzen zu können – mithilfe von Botnets und Webseiten verbreiten sie verborgene und Zero-Day-Malware. Zudem können einige Malware-Varianten bereits Gegenmaßnahmen auf Betriebssystemebene deaktivieren und PCs sowie Geräte mit fester Funktion unbrauchbar machen.

Die Situation der CIOs wird zusätzlich dadurch erschwert, dass sie den Energieverbrauch gerade nicht genutzter Desktop-Computer senken müssen, um Umweltvorschriften zu erfüllen. Es wäre hilfreich, gerade nicht verwendete Systeme auszuschalten. Gleichzeitig benötigen sie jedoch eine zuverlässige Möglichkeit, um Sicherheit und Compliance verwalten sowie IT-Prozesse wie Scans, Aktualisierungen oder Patch-Installationen zu Zeiten ausführen zu können, wenn die Produktivität der Mitarbeiter nicht eingeschränkt wird.

Hauptvorteile (Fortsetzung)

- **Verbesserung der Benutzerproduktivität:** Durchführung ressourcenintensiver Aufgaben außerhalb der Arbeitszeiten, um die Arbeit der Endbenutzer nicht zu beeinträchtigen
- **Reduzierung der IT-Kosten:** Vermeidung von häufigen Support-Besuchen am Arbeitsplatz sowie längeren Telefonaten mit dem Service-Personal
- **Senkung der Stromkosten von Endgeräten:** Implementierung eines Programms für Energieeinsparungen, ohne den Zugriff für Sicherheit oder Patch-Installation einzuschränken

Erkennung und Nutzung Ihrer Intel vPro-Plattformen

Mit der Software McAfee ePO Deep Command können Sie die Vorteile der Intel vPro-Technologie nutzen. Diese umfassen die Intel AMT Alarm Clock-Funktion, Fernaktivierung, die KVM-Funktion (Keyboard, Video, Mouse) sowie IDE Redirection. Mit dem McAfee ePO Deep Command Discovery and Reporting-Modul erkennen Sie Computer mit AMT in Ihrer Umgebung. Detaillierte Berichte zeigen, auf welchen PCs und Endgeräten Sie den McAfee ePO Deep Command-Agenten ausbringen sollten. Die Software McAfee ePO Deep Command optimiert auch die Bereitstellung von Intel AMT, um dessen Aktivierung zu vereinfachen. Sobald McAfee ePO Deep Command auf AMT-fähigen PCs und Endgeräten installiert ist, können Sie diese aus der Ferne auf Hardware-Ebene verwalten, ohne auf das Betriebssystem zugreifen zu müssen.

Die Antwort: Verwaltung aus der Ferne

Jetzt können Sicherheitsadministratoren mit ausgeschalteten, defekten oder verschlüsselten Endgeräten kommunizieren und sie auf Hardware-Ebene kontrollieren. Diese Verbindung zur Hardware ermöglicht die Fernverwaltung zur Durchsetzung von Sicherheits- oder Compliance-Richtlinien sowie die Senkung der Betriebskosten für Sicherheit. Neben einer besseren Sicherheitslage gewährleisten diese Kontrollen die Einführung von Energieverwaltungsprogrammen zur Senkung des Stromverbrauchs sowie den Zugriff auf die Endgeräte. Mithilfe der Intel vPro AMT-Technologie kann die Software McAfee ePO Deep Command auf Endgeräte zugreifen, ohne auf das Betriebssystem angewiesen zu sein. Dank dieses Zugriffs auf Hardware-Ebene können Administratoren Systeme

einschalten, Sicherheitsaufgaben ausführen und die Endgeräte anschließend wieder in den bisherigen Zustand zurückversetzen. McAfee ePO Deep Command ermöglicht sogar den abgesicherten Start des Boot-Vorgangs von Endgeräten mit der Software McAfee Complete Data Protection (für Endgeräteverschlüsselung), ohne dass dazu Benutzeranmeldeinformationen erforderlich sind, um Sicherheitsaufgaben per Fernzugriff durchzuführen. Diese Abläufe können automatisch per Zeitsteuerung oder manuell ausgelöst werden.

McAfee ePO Deep Command kommuniziert mit Endgeräten auf einer Ebene unterhalb des Betriebssystems. Zudem können Sie mithilfe der bekannten Verwaltungsplattform McAfee ePO schwierig zu verwaltende Endgeräte von einem zentralen Ort aus konfigurieren und wiederherstellen.

Aktivierung und Ausführung

Administratoren können Sicherheitsmaßnahmen oder zeitaufwändige Aufgaben außerhalb der normalen Arbeitszeiten durchführen, ohne die Arbeitsabläufe der Benutzer zu beeinträchtigen. Mithilfe von AMT Alarm Clock können Sicherheitsadministratoren Endgeräte einschalten und aus dem Ruhezustand wecken, selbst wenn diese verschlüsselt sind. Anschließend können sie beispielsweise folgende Sicherheitsaufgaben durchzuführen:

- Sicherheits- und Konfigurations-Updates (einschließlich DAT-Dateien)
- On-Demand-Scans
- Installation zusätzlicher Sicherheitsprodukte
- Berichte zu Ereignissen
- Patch-Installationen für Anwendungen oder das Betriebssystem

Systemanforderungen

- McAfee ePO 4.6 (Discovery and Reporting-Modul); McAfee ePO 4.6 Patch 6 (McAfee ePO Deep Command); McAfee ePO 5.0 und höher
- McAfee Agent 4.5 oder höher
- McAfee Drive Encryption 7.0 und höher (für Remote-Funktionen zur Verschlüsselungsverwaltung)
- Unterstützte Betriebssysteme: Microsoft Windows XP, Windows Vista, Windows 7, Windows 8, Windows Server 2003, Windows Embedded XP, Windows Embedded 7
- Unterstützt Intel vPro AMT ab Version 2.2
- Intel Setup and Configuration Software (SCS) 8.2 und höher

Wiederherstellung deaktivierter Endgeräte per Fernzugriff

Beim Auftreten von Problemen wie Betriebssystem- oder Laufwerkfehlern werden Administratoren und Benutzer die Vorteile der integrierten Verwaltung durch McAfee ePO Deep Command schnell zu schätzen wissen. Administratoren können sich per AMT lokal und per Fernzugriff mit defekten PCs, Endgeräten und KVM-Geräten (Keyboard, Video, Mouse) verbinden, um eine Problembehebung per Fernzugriff durchzuführen, beispielsweise den Neustart des Computers mithilfe eines alternativen, im Netzwerk gespeicherten ISO-Abbilds zu erzwingen. In den meisten Fällen muss das Endgerät nicht per Kabel mit dem Netzwerk verbunden sein, da McAfee ePO Deep Command auch abgesicherte Endgeräte verwalten kann, die per WLAN verbunden sind.

Die Intel AMT „Fast Call for Help“-Funktion erlaubt Benutzern, schnell und einfach Hilfe bei McAfee ePO-Administratoren anzufordern. Anschließend hat der McAfee ePO-Administrator folgende Möglichkeiten:

- Anweisung an das Endgerät, von einem Abbild aus einem anderen Speicherort im Netzwerk zu starten
- Vollständige Kontrolle des lokalen KVM
- Zurücksetzen des Benutzer-Verschlüsselungskennworts
- Bereinigung und Wiederherstellung infizierter, deaktivierter oder in Quarantäne befindlicher Systeme, ohne dass physischer Zugriff erforderlich ist

Sicherheit, die Bedrohungen einen Schritt voraus bleibt

Dank dieser umfassenden Kontrollen stehen den Sicherheitsteams neue Möglichkeiten zum Schutz von Endgeräten vor neuen Bedrohungen zur Verfügung. Systeme können noch vor dem Ausbruch einer potenziellen Bedrohung aktualisiert und Gegenmaßnahmen aus der Ferne aktiviert werden, um Auswirkungen auf die Mitarbeiterproduktivität zu vermeiden und die Sicherheit der Daten zu gewährleisten.

Senkung der Stromkosten von Endgeräten

Da Sie Endgeräte mit McAfee ePO Deep Command aus dem Ruhezustand hochfahren, die Richtlinien aktualisieren und die Endgeräte wieder in ihren ursprünglichen Betriebszustand versetzen können, erfüllen Sie Branchenvorgaben zur Senkung des Energieverbrauchs, ohne dabei die Sicherheit zu beeinträchtigen. Wenden Sie sich an McAfee, um mehr über mögliche Energieeinsparungen zu erfahren.

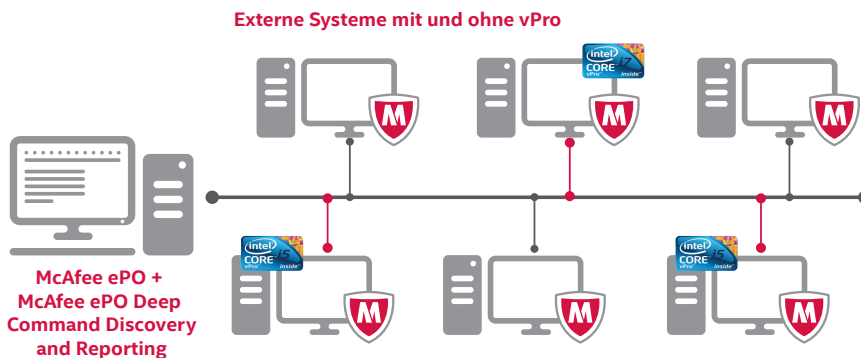


Abbildung 1. McAfee ePO Deep Command erkennt vPro-Systeme und stellt die Software zur Aktivierung von Intel AMT bereit.

Skalierbarkeit und Berichterstellung für Unternehmen

McAfee ePO Deep Command erweitert das Management-Framework von ePolicy Orchestrator® (McAfee ePO™), das hunderttausende Endgeräte verwalten kann. Durch die Unterstützung verteilter Architekturen und Sicherheitsteams bietet McAfee ePO eine zentrale Umgebung zur Sicherheitsrichtlinienverwaltung und Berichterstellung für die gesamte McAfee-Sicherheitsinfrastruktur, sodass Sie Richtlinien sowie Compliance über das Betriebssystem hinaus ausdehnen können. Durch den Umfang der Informationen, die Sie in McAfee ePO-Dashboards und -Berichte aufnehmen können, verbessert sich der Compliance-Überblick der einzelnen Endgeräte sowie die Sicherheitslage des gesamten Unternehmens. Zudem werden Audits durch Datenkorrelierung leicht gemacht.

Weitere Informationen finden Sie unter www.mcafee.com/de/products/epo-deep-command.aspx.

McAfee ePO Deep Command ist als eigenständige Software verfügbar, aber auch in den McAfee Complete Data Protection-Suites enthalten. Weitere Informationen finden Sie unter www.mcafee.com/de/products/data-protection/index.aspx.

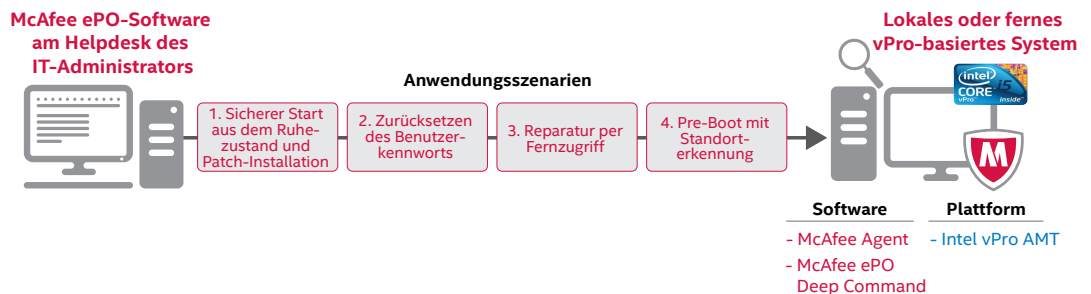


Abbildung 2. Dank McAfee ePO Deep Command kann das Helpdesk verschiedene Aufgaben lokal sowie per Fernzugriff durchführen.



McAfee. Part of Intel Security.

Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 37 07-0
www.intelsecurity.com

1. McAfee ePO Deep Command ist als eigenständige Software verfügbar, aber auch in den McAfee Complete Data Protection-Suites enthalten. Weitere Informationen finden Sie unter www.mcafee.com/de/products/data-protection/index.aspx.