



McAfee Complete Data Protection – Advanced

Umfassender Datenschutz – jederzeit und überall

Sensible Daten unterliegen ständig der Gefahr von Verlust, Diebstahl oder Offenlegung. Oft werden die Daten dabei einfach auf einem Laptop oder USB-Gerät aus dem Unternehmen getragen. Unternehmen, in denen es zu solchen Datenlecks kommt, riskieren ernsthafte Konsequenzen wie Geldstrafen, die Veröffentlichung des Datenschutzverstoßes, Image- und Vertrauensverlust sowie finanzielle Einbußen. Laut einem Bericht des Ponemon Institute gehen 7 Prozent aller Unternehmens-Laptops während ihrer Nutzungsdauer verloren oder werden gestohlen.¹ Die starke Verbreitung von Mobilgeräten mit großen Speicherkapazitäten und Internetzugriff ergibt noch mehr Möglichkeiten für Datenkompromittierung oder Diebstahl, sodass der Schutz vertraulicher, proprietärer und personenbezogener Informationen höchste Priorität erhalten sollte. McAfee® Complete Data Protection – Advanced löst all diese Probleme – und noch viele weitere.

Wichtige Funktionen

- McAfee Data Loss Prevention Endpoint
- McAfee Device Control
- Drive Encryption
- File and Removable Media Protection
- Management of Native Encryption
- McAfee ePO Deep Command

Hauptvorteile

- Verschaffen Sie sich Kontrolle über Ihren Datenbestand, indem Sie überwachen und regeln, wie Ihre Mitarbeiter auf Daten zugreifen, diese verwenden und über gängige Kanäle wie E-Mail, Instant Messaging (IM), Ausdrücke und USB-Laufwerke übertragen – sowohl im Büro als auch unterwegs.
- Stoppen Sie Datenverluste durch hochentwickelte Malware, die vertrauliche und persönliche Informationen abfängt.
- Sichern Sie auf Desktop-Rechnern, Laptops, Tablets und in der Cloud gespeicherte Daten.
- Verwalten Sie die systemeigene Verschlüsselung von Apple FileVault und Microsoft BitLocker auf Endgeräten direkt aus McAfee ePO.

Schutz vor Datenkompromittierung für stärkere Kontrolle

Der erste Schritt beim Schutz vor Datenkompromittierung am Endgerät besteht darin, eine bessere Übersicht und Kontrolle über Ihre Daten zu schaffen, selbst wenn diese versteckt sind. Mit McAfee Complete Data Protection – Advanced können Sie unternehmensweite Sicherheitsrichtlinien erstellen und durchsetzen, die Ihren Mitarbeitern Regeln und Beschränkungen für die Verwendung von vertraulichen Daten auferlegen. Dies gilt auch für die Datenübertragung über gängige Kanäle wie E-Mail, Instant Messenger, Drucker oder USB-Laufwerke. Ob Ihre Mitarbeiter im Büro, zuhause oder unterwegs sind, spielt dabei keine Rolle.

Unternehmensgerechte Geräteverschlüsselung

Sichern Sie Ihre vertraulichen Daten mit einer unternehmensgerechten Sicherheitslösung ab, die nach FIPS 140-2 und Common Criteria EAL2+ zertifiziert und durch den Intel® Advanced Encryption Standard mit Intel AES-NI beschleunigt wird. McAfee Complete Data

Protection – Advanced setzt auf Festplattenverschlüsselung in Kombination mit einer starken Zugangskontrolle über Zwei-Faktor-Pre-Boot-Authentifizierung zum Schutz vor unbefugten Zugriffen auf vertrauliche Daten auf allen Endgeräten, darunter Desktop-Computer, VDI-Workstations, Laptops, USB-Geräte, CDs/DVDs usw.

Verschlüsselung von Wechselmedien, Dateien, Ordnern und Cloud-Speicher

Stellen Sie sicher, dass bestimmte Dateien und Ordner immer verschlüsselt sind – selbst dann, wenn sie gerade bearbeitet, kopiert oder gespeichert werden. Bei McAfee Complete Data Protection – Advanced werden die von Ihnen gewählten Dateien und Ordner automatisch, transparent und im laufenden Betrieb verschlüsselt, bevor sie in Ihrem Unternehmen bewegt werden. Sie können für einzelne Benutzer und Benutzergruppen zentrale Richtlinien aufstellen und durchsetzen, um die Verschlüsselung bestimmter Dateien und Ordner ohne Zutun des Benutzers zu erzwingen.

Hauptvorteile (Fortsetzung)

- Kontrollieren Sie Ihre Endgeräte auf Hardware-Ebene unabhängig davon, ob diese ausgeschaltet, defekt oder verschlüsselt sind. Auf diese Weise vermeiden Sie Support-Besuche am Arbeitsplatz und endlose Helpdesk-Telefonate aufgrund von Sicherheitszwischenfällen, Virenausbrüchen oder vergessenen Kennwörtern.
- Weisen Sie mithilfe fortschrittlicher Reporting- und Audit-Funktionen gegenüber Prüfern und anderen Verantwortlichen die Compliance mit internen und gesetzlichen Datenschutzanforderungen nach. Dazu werden Ereignisse überwacht und detaillierte Berichte erstellt.

Funktionen von McAfee ePO Deep Command

- Schnellere Problembekämpfung
- Verwaltung der Problembekämpfung per Fernzugriff auf beliebigen Computern überall auf der Welt durch Zugriff auf die Hardware
- Verbesserung der Benutzerproduktivität
- Durchführung ressourcenintensiver Aufgaben außerhalb der Arbeitszeiten, um die Arbeit der Endbenutzer nicht zu beeinträchtigen
- Senkung der IT-Kosten durch Verringerung der Support-Besuche am Arbeitsplatz sowie längerer Telefonate mit dem Service-Personal
- Senkung der Energiekosten durch Umsetzung von Energiesparprogrammen, ohne den Zugriff für Sicherheitsmaßnahmen und Patches zu beeinträchtigen
- Schnelle Erkennung und Bereitstellung von Intel vPro AMT durch einfache Identifizierung von PCs mit Intel vPro und anschließende Aktivierung von Intel AMT zur einfachen Nutzung des Fernzugriffs

Management of Native Encryption

Mit Management of Native Encryption können Sie die integrierten Verschlüsselungsfunktionen von Apple FileVault für Mac OS X und Microsoft BitLocker für Windows-Plattformen direkt über die Software McAfee® ePolicy Orchestrator® (McAfee ePO™) verwalten. Management of Native Encryption bietet daher von Anfang an Kompatibilität mit OS X- und Windows-Patches, Upgrades, Firmware-Aktualisierungen von Apple sowie Support auch für neue Apple-Hardware. Wenn Benutzer FileVault bzw. BitLocker bereits aktiviert haben, können Administratoren mit Management of Native Encryption die Wiederherstellungsschlüssel manuell importieren.

Out-of-Band-Fernverwaltung zur Senkung der Betriebskosten

McAfee ePO Deep Command nutzt die Funktion Intel® vPro Active Management Technology (Intel vPro AMT) zur Senkung der Betriebskosten, zur Verbesserung von Sicherheit und Compliance sowie zur Vereinfachung der Problembekämpfung per Fernzugriff. Die Software McAfee ePO Deep Command kann PCs aus dem Ruhezustand hochfahren, Richtlinien aktualisieren und Computer wieder in den Energiesparmodus versetzen.²

Zentrale Sicherheitsverwaltung und erweiterte Berichtsfunktionen

Richten Sie mit der zentralen McAfee ePO-Konsole verbindliche, unternehmensweite Sicherheitsrichtlinien dazu ein, wie Daten verschlüsselt, überwacht und vor Verlust geschützt werden, und erzwingen Sie diese. Sie können Sicherheitsrichtlinien zur Verschlüsselung, Filterung und Überwachung vertraulicher Daten und zur Blockierung unbefugter Zugriffe darauf definieren, einrichten, verwalten und aktualisieren.

Funktionen von McAfee Complete Data Protection – Advanced

Gerätesteuerung

- Überwachung und Kontrolle darüber, wie Mitarbeiter Daten auf Wechselmedien übertragen können – selbst wenn sie nicht mit dem Unternehmensnetzwerk verbunden sind

Schutz vor Datenkompromittierung

- Kontrolle darüber, wie Benutzer auf (physischen oder virtuellen) Endgeräten mithilfe von Anwendungen und auf Speichergeräten vertrauliche Daten versenden, nutzen und drucken
- Vermeidung der Kompromittierung vertraulicher Daten durch Trojaner, Würmer oder Filesharing-Anwendungen, die Zugangsdaten Ihrer Mitarbeiter abfangen
- Schutz aller Daten, Formate und Ableitungen, selbst wenn diese verändert, kopiert, eingefügt, komprimiert oder verschlüsselt wurden

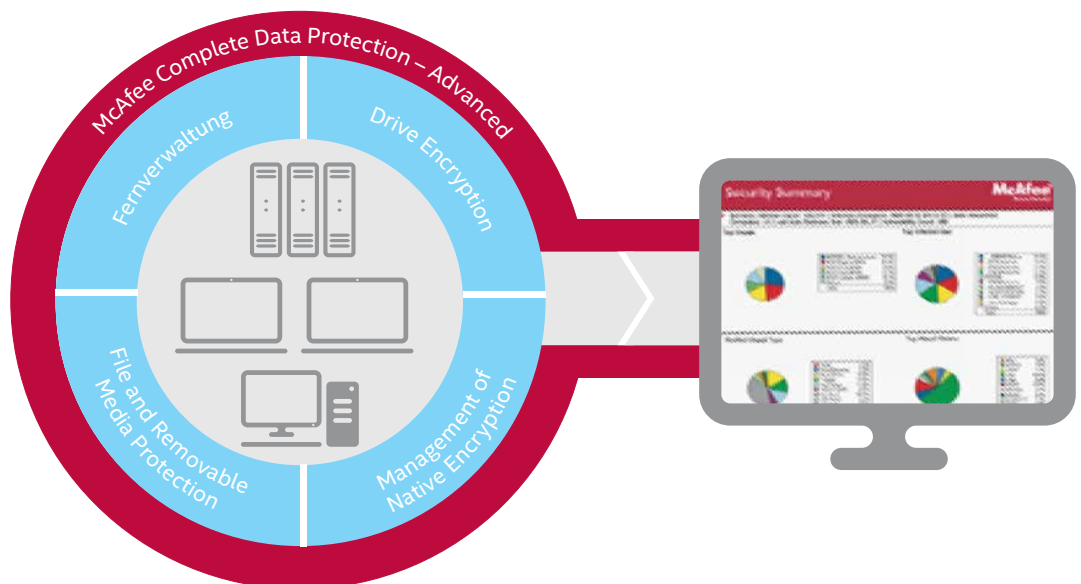


Abbildung 1. McAfee Complete Data Protection – Advanced

Spezifikationen von McAfee Complete Data Protection – Advanced

Microsoft Windows-Betriebssysteme

- Microsoft Windows 7, 8 und 10 (32-Bit- und 64-Bit-Versionen)
- Microsoft Windows Vista (32-Bit- und 64-Bit-Version)
- Microsoft Windows XP (nur 32-Bit-Version)
- Microsoft Windows Server 2008
- Microsoft Windows Server 2003 (nur 32-Bit-Version)

Hardware-Anforderungen

- Prozessor: Laptop- und Desktop-Computer mit Pentium III (1 GHz oder höher)
- RAM: mindestens 512 MB (1 GB empfohlen)
- Festplatte: mindestens 200 MB freier Speicherplatz

Apple Mac-Betriebssysteme

- Mac OS X El Capitan, Yosemite, Mountain Lion und Mavericks

Hardware-Anforderungen

- Prozessor: Intel-basierter Mac-Laptop mit 64-Bit-EFI
- RAM: mindestens 1 GB
- Festplatte: mindestens 200 MB freier Speicherplatz

Zentrale Verwaltung

- Die technischen Spezifikationen entnehmen Sie bitte dem Datenblatt zur McAfee ePO-Plattform.

Spezifikationen von McAfee ePO Deep Command

- Unterstützung für Intel vPro AMT 6.1.2, 7.0, 7.1.4 und 8.0 Intel SCS (Setup and Configuration Software) 8.2

Unternehmensgerechte Laufwerkverschlüsselung

- Automatische Verschlüsselung ganzer Geräte ohne Zutun der Benutzer und ohne Anwenderschulungen durchführen oder Einbußen bei den Systemressourcen hinnehmen zu müssen
- Überprüfung der Identität befugter Benutzer mit starker Mehrfaktor-Authentifizierung

Verschlüsselung von Wechselmedien

- Automatische Echtzeit-Verschlüsselung für fast alle mobilen privaten oder vom Unternehmen gestellten Speichergeräte
- Zugriff auf verschlüsselte Daten unabhängig vom Standort des Benutzers und ohne zusätzliche Software

Verschlüsselung von Dateien, Ordnern und Cloud-Speicher

- Sichere Speicherung der Dateien und Ordner unabhängig vom Speicherort, einschließlich lokale Festplatten, Datei-Server, Wechselmedien sowie Cloud-Speicher wie Box, Dropbox, Google Drive und Microsoft OneDrive

Verwaltung der integrierten Verschlüsselung auf Mac- und Windows-Geräten

- Verwaltung von FileVault auf jeder beliebigen Mac-Hardware, die Mac OS X Mountain Lion, Mavericks, Yosemite oder El Capitan ausführen kann, direkt aus McAfee ePO
- Verwaltung von BitLocker auf Systemen mit Windows 7, 8 und 10 direkt aus McAfee ePO, ohne dass dazu ein separater MBAM-Server (Microsoft BitLocker Management and Administration) erforderlich ist

Out-of-Band-Fernverwaltung

- Fernverwaltung von PCs über das Betriebssystem hinaus auf Hardware-Ebene
- Einschalten auch verschlüsselter PCs bzw. Wecken aus dem Ruhezustand zur Durchführung von Sicherheitsaufgaben

Zentrale Verwaltungskonsole

- Verwendung der Infrastrukturverwaltungs-Software McAfee ePO zur Verwaltung der Verschlüsselung ganzer Laufwerke, Wechselmedien, Dateien und Ordner, zur Richtlinienkontrolle und Patch-Verwaltung, Wiederherstellung verloren gegangener Kennwörter und für den Nachweis der Vorschrifteneinhaltung
- Synchronisierung von Sicherheitsrichtlinien mit Microsoft Active Directory, Novell NDS, PKI u. a.
- Nachweis der Geräteverschlüsselung dank umfassender Audit-Funktionen
- Protokollierung der Datenübertragungen zur Aufzeichnung von Informationen wie Absender, Empfänger, Zeitstempel, Datenspuren sowie Datum und Uhrzeit der letzten erfolgreichen Anmeldung

Weitere Informationen zu McAfee-Datenschutzlösungen finden Sie unter www.mcafee.com/de/products/data-protection/index.aspx.



McAfee. Part of Intel Security.

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

1. *The Billion Dollar Lost Laptop Problem Study* (Studie zu verlorenen Laptops mit Milliardenwerten), Ponemon Institute, September 2010.
2. *Keep Your Client PCs Safer, Wherever They Go* (Besserer Schutz für Ihre Client-PCs an jedem Ort), <http://www.mcafee.com/de/resources/solution-briefs/sb-keep-your-client-pcs-safer.pdf>