

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. Die starke Verbreitung von Mobilgeräten mit großen Speicherkapazitäten und Internetzugang ergibt noch mehr Möglichkeiten für Datenkompromittierung oder Diebstahl, sodass der Schutz vertraulicher, proprietärer und personenbezogener Informationen höchste Priorität erhalten sollte. Die McAfee® Complete Data Protection – Advanced-Suites lösen all diese Probleme – und noch viele weitere.

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 ist sowie durch Intel Advanced Encryption Standard – New Instructions (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 (virtuelle Desktop-Infrastrukturen), Laptops, USB-Geräte, CDs/DVDs usw.

Wichtige Funktionen

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

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 Messenger, Ausdrucke und USB-Laufwerke übertragen – sowohl im Büro als auch unterwegs.
- Stoppen Sie Datenverluste durch hochentwickelte Malware, die vertrauliche und persönliche Informationen abfängt.

Folgen Sie uns



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.

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 MVISION ePO oder McAfee® ePolicy Orchestrator® (McAfee ePO™) verwalten. Management of Native Encryption bietet von Anfang an Kompatibilität mit Apple OS X- und Microsoft Windows-Patches, Upgrades, Firmware-Aktualisierungen von Apple sowie Support für neue Apple-Hardware. Wenn Benutzer FileVault bzw. BitLocker bereits aktiviert haben, können Administratoren mit Management of Native Encryption die Wiederherstellungsschlüssel manuell importieren.

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 der McAfee Complete Data Protection – Advanced-Suite

Gerätesteuerung

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

Schutz vor Datenverlust

- Kontrolle darüber, wie Benutzer vertrauliche Daten auf (physischen oder virtuellen) Endgeräten mithilfe von Anwendungen versenden, nutzen und drucken sowie auf Speichergeräte übertragen
- 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

Hauptvorteile (Fortsetzung)

- 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 MVISION ePO oder McAfee ePO.
- 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 Ihre Compliance mit hochentwickelten Berichts- und Audit-Funktionen nach. Überwachen Sie Vorfälle, und erstellen Sie detaillierte Berichte, die Prüfern und anderen Verantwortlichen Ihre Compliance mit internen und gesetzlichen Datenschutzerfordernungen zeigen.

Unternehmensgerechte Laufwerkverschlüsselung

- Automatische Verschlüsselung ganzer Geräte ohne Zutun der Benutzer ohne Anwenderschulungen durchführen oder Einbußen bei den Systemressourcen hinnehmen zu müssen
- Überprüfung der Identität befugter Benutzer mit starker Mehrfaktor-Authentifizierung
- Unterstützung für Intel Software Guard Extension (Intel SGX)
- Mit Drittanbietern für Anmeldeinformationen kompatibel
- Integrierte Upgrade-Unterstützung für Windows 10 Anniversary Update

Verschlüsselung von Wechselmedien

- Automatische Echtzeit-Verschlüsselung für fast alle mobilen privaten oder vom Unternehmen gestellten Wechselspeichergeräte
- 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

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)
 - Arbeitsspeicher: 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
 - Arbeitsspeicher: mindestens 1 GB
 - Festplatte: mindestens 200 MB freier Speicherplatz
- Zentrale Verwaltung

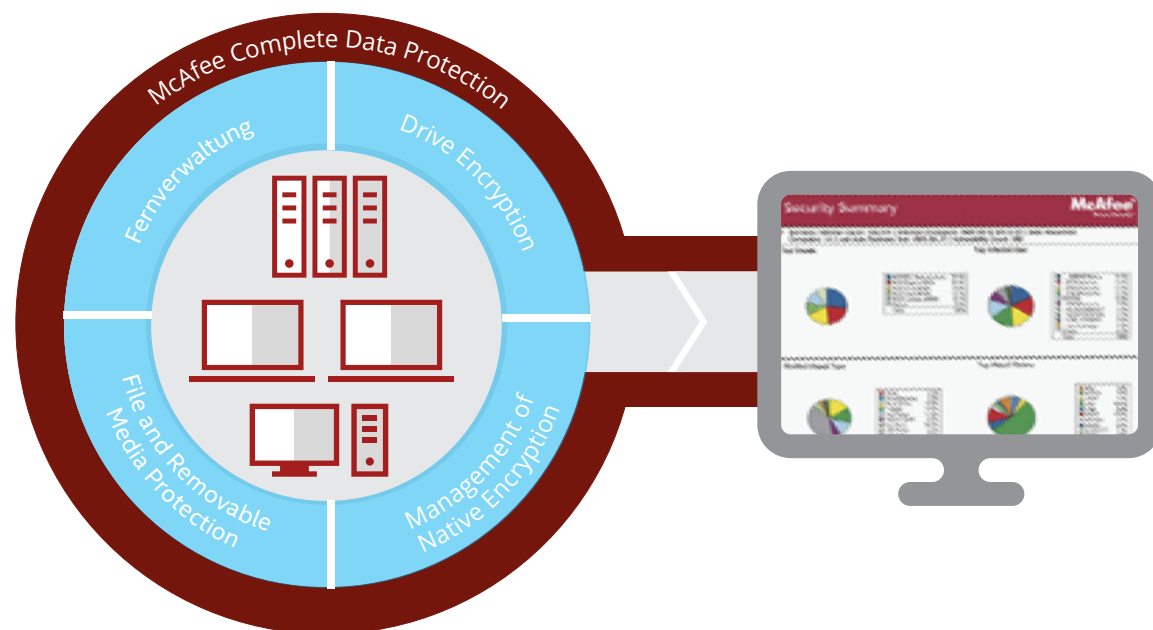


Abbildung 1. McAfee Complete Data Protection

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 und El Capitan ausführen kann, direkt aus MVISION ePO oder McAfee ePO
- Verwaltung von BitLocker auf Systemen mit Windows 7, 8 und 10 direkt aus MVISION ePO oder McAfee ePO, ohne dass dazu ein separater MBAM-Server (Microsoft BitLocker Management and Administration) erforderlich ist

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

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



Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 3707 0
www.mcafee.com/de

McAfee, das McAfee-Logo, ePolicy Orchestrator und McAfee ePO sind Marken oder eingetragene Marken von McAfee, LLC oder seinen Tochterunternehmen in den USA und anderen Ländern. Alle anderen Namen und Marken sind Eigentum der jeweiligen Besitzer.
Copyright © 2019 McAfee, LLC. 4376_1019
OKTOBER 2019