



McAfee® Total Protection for Data

Umfassender Schutz für Ihre wichtigen Daten

In den vergangenen Jahren hat das Durchsickern sensibler Kundendaten in der Öffentlichkeit wiederholt für Schlagzeilen gesorgt. Oft sind die Daten dabei schlicht und ergreifend auf einem Laptop oder einem anderen mobilen Gerät offen aus dem Unternehmen getragen worden. Unternehmen, in denen es zu solchen Datenlecks kommt, riskieren ernste Konsequenzen, darunter Geldstrafen, die Offenlegung des Datenschutzverstoßes, Image- und Vertrauensverlust sowie finanzielle Einbußen. 2007 betrug die durchschnittlichen Folgekosten für ein Unternehmen, das einen Datenschutzverstoß hinnehmen musste, 6,3 Millionen Dollar.¹

In der heutigen Arbeitsumgebung, in der das Internet allgegenwärtig ist und die Zahl von Mobilgeräten rapide ansteigt, muss dem Schutz vertraulicher Kundeninformationen und geistigen Eigentums oberste Priorität eingeräumt werden.

HAUPTVORTEILE

Schutz vor Datenverlust

- Einsatz zentral verwalteter Sicherheitsrichtlinien zur Regelung, wie Mitarbeiter auf vertrauliche Daten zugreifen, sie verwenden und übertragen dürfen

Geräteverschlüsselung auf Unternehmensniveau

- Schutz vertraulicher Daten auf allen Endgeräten durch Verschlüsselung ganzer Laufwerke in Kombination mit strengen Zugriffskontrollen

Dauerhafte Verschlüsselung von Dateien und Ordnern

- Automatische, transparente Verschlüsselung von Dateien im laufenden Betrieb, bevor sie an andere Stellen in Ihrem Unternehmen gelangen

Zentrale Management-Konsole

- Festlegung firmeneigener Sicherheitsrichtlinien zur Kontrolle, wie sensible Daten verschlüsselt, überwacht und vor Verlust geschützt werden
- Geringerer Zeit-, Verwaltungs- und Schulungsaufwand für höheren ROI und niedrigere TCO

Fortschrittliche Reporting- und Prüffunktionen

- Echtzeit-Überwachung von Vorfällen und Erzeugung detaillierter Berichte
- Nachweis von Maßnahmen zur Einhaltung interner und gesetzlicher Richtlinien gegenüber Auditoren, Vorstandsmitgliedern und anderen Interessengruppen

McAfee Total Protection for Data

McAfee® Total Protection for Data ist branchenweit die kompletteste Lösung zum Schutz Ihrer vertraulichen Daten. Unbefugte Zugriffe auf und Übertragungen von sensiblen Informationen werden durch starke Verschlüsselungsmaßnahmen, Authentifizierung, Schutz vor Datenverlust und richtliniengestützte Sicherheitskontrollen verhindert – überall und jederzeit.

Schutz vor Datenverlust

Der erste Schritt beim Schutz vor Datenverlust besteht darin, eine bessere Übersicht und Kontrolle über Ihre Daten zu schaffen, selbst wenn diese versteckt sind. Mit McAfee Total Protection for Data können sie unternehmensweite Sicherheitsrichtlinien aufstellen und durchsetzen, die Ihren Mitarbeitern Regeln und Beschränkungen für die Verwendung von sensiblen Daten sowie für die Datenübertragung auf gängigen Wegen wie E-Mail, Instant Messenger, Druck oder USB-Laufwerke vorgeben. Ob Ihre Mitarbeiter am Arbeitsplatz, zuhause oder unterwegs sind, spielt dabei keine Rolle. Die Kontrolle bleibt in Ihren Händen.

Geräteverschlüsselung auf Unternehmensniveau

Schützen Sie Ihre vertraulichen Daten mit einer Sicherheitslösung auf Unternehmensniveau. Total Protection for Data setzt auf die Verschlüsselung ganzer Festplatten in Kombination mit einer strengen Zugangskontrolle über Zwei-Faktor-Pre-Boot-Authentifizierung zum Schutz vor unbefugten Zugriffen auf vertrauliche Daten auf allen Endgeräten, darunter Laptops, Handheld-Geräte, Smartphones usw.

Dauerhafte, transparente Verschlüsselung von Dateien und Ordnern

Stellen Sie sicher, dass bestimmte Dateien und Ordner ständig verschlüsselt sind, egal, wo Daten bearbeitet, kopiert oder gespeichert werden – auch auf Desktops, Laptops, Handheld-Geräten, Smartphones und anderen Geräten. Bei Total Protection for Data werden die von Ihnen gewählten Dateien und Ordner transparent und im laufenden Betrieb verschlüsselt, bevor sie an andere Stellen in Ihrem Unternehmen gelangen. Sie können für einzelne Anwender und Anwendergruppen zentrale Richtlinien aufstellen und durchsetzen, um die Verschlüsselung bestimmter Dateien und Ordner ohne Zutun des Anwenders zu erzwingen.

Zentrales Sicherheitsmanagement und fortschrittliches Reporting

Die Integration von Total Protection for Data in ePolicy Orchestrator® (ePO™) ist für 2008 geplant². Mit dieser Integration wird nicht nur zentrales, richtliniengestütztes Sicherheitsmanagement ermöglicht, sondern es werden auch fortschrittliche Reportingfunktionen bereitgestellt, die Ihnen dabei helfen, strenge gesetzliche und branchenspezifische Datenschutzvorschriften zu erfüllen, "Safe Harbor"-Datenschutz zu gewährleisten und gegenüber internen wie externen Auditoren, Vorstandsmitgliedern und anderen wichtigen Interessengruppen die Einhaltung von Richtlinien nachzuweisen.

SYSTEMANFORDERUNGEN

ePO-Server

Betriebssysteme

- Microsoft® Server 2003 SP1, 2003 R2

Hardware-Anforderungen

- Festplattenspeicher: 250 MB
- RAM: 512 MB
1 GB empfohlen
- Prozessor – entsprechend Pentium II oder höher - min. 450 MHz

Desktop- und Laptop-Endgeräte

Betriebssysteme

- Microsoft® Windows Vista* (alle 32- und 64-bit-Versionen)
- Microsoft® Windows XP Professional SP1 oder höher
- Microsoft® Windows 2000 SP4 oder höher

* 2008 für DLP erhältlich²

Hardware-Anforderungen

- Prozessor: Pentium III 1 GHz oder höher
- RAM: 512 MB empfohlen
- Festplattenspeicher: min. 200 MB
- Netzwerkanschluss: TCP/IP für Remote-Zugriff

Windows Mobile-Endgeräte

Betriebssysteme

- Microsoft® Windows Mobile 6.0 for Smartphone
- Microsoft® Windows Mobile 6.0 for PDA
- Microsoft® Windows Mobile 5.0 for Smartphone
- Microsoft® Windows Mobile 5.0 for Pocket-PC

Hardware-Anforderungen

- Prozessor: min. 195 MHz
- RAM: 64 MB
- Netzwerkanschluss: TCP/IP für Remote-Zugriff und Activesync 4.5 oder höher für kabelgebundene Richtlinien-Installation/-Aktualisierung

Funktionen

Schutz vor Datenverlust

- Erhalten Sie die Kontrolle darüber, wie Benutzer über das Netzwerk, durch Anwendungen und auf Speichergeräten vertrauliche Daten versenden, einsehen und drucken können: Schützen Sie E- und Web-Mail, Peer-to-Peer (P2P)-Anwendungen, Instant Messenger, Skype, HTTP, HTTPS, FTP, Wi-Fi, USB, CD, DVD, Drucker, Faxgeräte und externe Speichermedien.
- Schützen Sie sich vor dem Verlust vertraulicher Daten durch Trojaner, Würmer oder Filesharing-Anwendungen, die ohne das Wissen Ihrer Mitarbeiter deren Zugangsdaten übernehmen.
- Schützen Sie alle Daten, Formate und Ableitungen, selbst wenn Daten verändert, kopiert, eingefügt, komprimiert oder verschlüsselt wurden – ohne Beeinträchtigung normaler Arbeitsabläufe.

Geräteverschlüsselung auf Unternehmensniveau

- Verschlüsseln Sie ganze Geräte ohne Zutun der Anwender und ohne Anwenderschulungen durchführen oder Einbußen bei den Systemressourcen befürchten zu müssen.
- Bei der Verschlüsselung ganzer Laufwerke werden viele Standard-Algorithmen wie AES-256 und RC5-1024 unterstützt.
- Überprüfen Sie die Identität befugter Anwender mit einer strengen Mehrfaktor-Authentifizierung.

Dauerhafte Verschlüsselung von Dateien und Ordnern

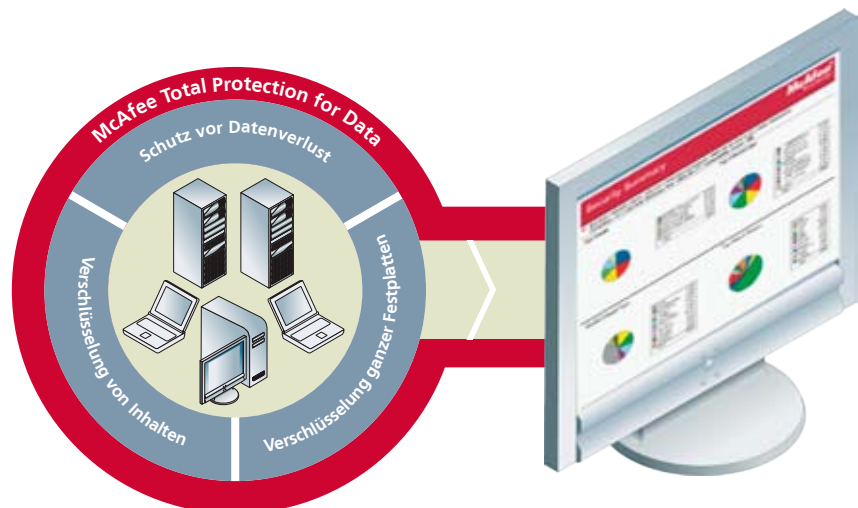
- Stellen Sie sicher, dass Dateien durch die Hinzufügung eines Datei-Headers, der jeder Bewegung der geschützten Datei folgt, auch dann verschlüsselt bleiben, wenn sie gerade nicht verwendet werden.
- Bewahren Sie Dateien und Ordner stets sicher auf, egal, ob sie auf lokalen Festplatten, Dateiservern oder Wechselmedien gespeichert sind – oder sogar als E-Mail-Anhänge.

Zentrale Management-Konsole

- Verwenden Sie ePO für detaillierte, inhaltsbasierte Filterung sowie zur Überwachung und Sperrung von unbefugten Zugriffen auf vertrauliche Daten.
- Verwalten Sie die Verschlüsselung ganzer Laufwerke sowie einzelner Dateien und Ordner, kontrollieren Sie das Richtlinien- und Patch-Management, stellen Sie verloren gegangene Schlüssel wieder her und weisen Sie die Einhaltung gesetzlicher Vorgaben nach.
- Synchronisieren Sie Sicherheitsrichtlinien mit Microsoft Active Directory, Novell NDS, PKI usw.

Fortschrittliche Reporting- und Prüffunktionen

- Nutzen Sie die umfassenden Auditfunktionen zum Beweis, dass Geräte verschlüsselt sind.
- Protokollieren Sie Datenübertragungen zur Aufzeichnung von Informationen wie Absender, Empfänger, Zeitstempel, Datenspur, Datum und Uhrzeit der letzten erfolgreichen Anmeldung, Datum und Uhrzeit des letzten empfangenen Updates sowie eine Angabe, ob die Verschlüsselung erfolgreich war oder nicht.



McAfee Total Protection for Data

Weitere Informationen zum Thema Datenschutz finden Sie im Internet unter www.mcafee.com/data_protection.

McAfee GmbH

Ohmstraße 1, D-85716 Unterschleißheim, Telefon: 089-3707 0 | Sachsenfeld 2, D-20097 Hamburg, Telefon: 040-2531-0
www.mcafee.de

McAfee und/oder andere genannte McAfee-Produkte in diesem Dokument sind eingetragene Marken oder Marken von McAfee, Inc. und/oder seinen Niederlassungen in den USA und/oder anderen Ländern. Das McAfee-Rot in Verbindung mit Sicherheit steht unverkennbar für alle McAfee Markenprodukte. Alle anderen nicht zu McAfee gehörenden Produkte sowie eingetragene und/oder nicht eingetragene Marken in diesem Dokument werden nur als Referenz genannt und sind Eigentum ihrer jeweiligen Rechtsinhaber.
© 2008 McAfee, Inc. Alle Rechte vorbehalten. 1-dp-tpd-001-0108