

McAfee Total Protection for Data

Umfassender Schutz für Ihre unternehmenskritischen Daten

In den vergangenen Jahren hat das Durchsickern vertraulicher Kundendaten in der Öffentlichkeit wiederholt für Schlagzeilen gesorgt. Oft sind die Daten dabei einfach auf einem Laptop oder einem anderen mobilen Gerät aus dem Unternehmen getragen worden. Unternehmen, in denen es zu solchen Datenlecks kommt, riskieren ernsthafte Konsequenzen wie Geldstrafen, die Veröffentlichung des Datenschutzverstößes, Image- und Vertrauensverlust sowie finanzielle Einbußen. 2008 betrug die durchschnittlichen Folgekosten von Datenschutzverstößen für Unternehmen 6,65 Millionen Dollar.¹

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

Hauptvorteile

Schutz vor Datenverlust

- Setzen Sie zentral verwaltete Sicherheitsrichtlinien ein, um festzulegen, wie Mitarbeiter auf vertrauliche Daten zugreifen, sie verwenden und übertragen dürfen

Unternehmensgerechte Geräteverschlüsselung

- 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 und Ordnern im laufenden Betrieb, bevor sie im Unternehmen bewegt werden

Zentrale Management-Konsole

- Legen Sie firmeneigene Sicherheitsrichtlinien fest, um zu steuern, wie vertrauliche Daten verschlüsselt, überwacht und vor Verlust geschützt werden
- Senken Sie den Zeit-, Verwaltung- und Schulungsaufwand für höhere Rendite und niedrigere Gesamtbetriebskosten

Fortschrittliche Reporting- und Prüffunktionen

- Echtzeit-Ereignisüberwachung und Erstellung 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 eine der vollständigsten Lösungen zum Schutz Ihrer vertraulichen Daten. Durch leistungsfähige Verschlüsselung, Authentifizierung, Schutz vor Datenverlusten und richtlinienbasierte Sicherheitskontrollen wird der unbefugte Zugriff auf vertrauliche Daten sowie deren Übertragung 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 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. Sie behalten die Kontrolle.

Unternehmensgerechte Geräteverschlüsselung

Schützen Sie Ihre vertraulichen Daten mit einer unternehmensgerechten Sicherheitslösung. Total Protection for Data verwendet 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, einschließlich Laptops, Handheld-Geräten, 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 – auf Desktops, Laptops, Handheld-Geräten, Smartphones usw. Bei Total Protection for Data 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 Anwender und Anwendergruppen zentrale Richtlinien erstellen und durchsetzen, um die Verschlüsselung bestimmter Dateien und Ordner ohne Zutun des Anwenders durchzusetzen.

Zentrales Sicherheitsmanagement und fortschrittliches Reporting

McAfee Total Protection for Data ist in den McAfee ePolicy Orchestrator® (McAfee ePO™) integriert, um die laufenden Kosten für Verwaltung, Bereitstellung, Reporting und Audits zu reduzieren. Diese Integration ermöglicht es Ihnen, ständig wechselnde Datenschutzbestimmungen effektiv einzuhalten, kontinuierlichen Schutz zu gewährleisten und die Einhaltung gegenüber internen und externen Auditoren und anderen Interessengruppen nachzuweisen. Außerdem ermöglicht sie ein zentrales, richtlinienbasiertes Sicherheitsmanagement. Die Integration stellt auch fortschrittliche Reportingfunktionen bereit, die Ihnen dabei helfen, strenge gesetzliche und branchenspezifische Datenschutzvorschriften zu erfüllen. "Safe Harbor"-Datenschutz wird gewährleistet um gegenüber internen wie externen Auditoren, Vorstandsmitgliedern und anderen Interessengruppen die Einhaltung von Richtlinien nachzuweisen.

¹ 2008 durchgeführte Studie des Ponemon Institute zu Kosten von Datenverlusten (Cost of Data Breach Study)

Systemanforderungen

ePO-Server

Betriebssysteme

- Microsoft Server 2003 SP1, 2003 R2

Hardware-Anforderungen

- Freier Festplattenspeicher: 250 MB
- RAM: 512 MB
1 GB RAM (empfohlen)
- Prozessor - Intel Pentium II-Klasse oder höher - mindestens 450 MHz

Desktop- und Laptop-Endgeräte

Betriebssysteme

- Microsoft Windows Vista* (alle 32- und 64-Bit-Versionen)
- Microsoft Windows XP Professional ab SP1
- Microsoft Windows 2000 ab SP4
* 2008 für DLP erhältlich

Hardware-Anforderungen

- Prozessor: Pentium III 1 GHz oder höher
- RAM: 512 MB (empfohlen)
- Freier Festplattenspeicher: mindestens 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: mindestens 195 MHz
- RAM: 64 MB
- Netzwerkanschluss: TCP/IP für Remote-Zugriff und ActiveSync ab 4.5 für kabelgebundene Richtlinieninstallation/-aktualisierung

Funktionen

Schutz vor Datenverlust

- Erhalten Sie Kontrolle darüber, wie Anwender über das Netzwerk, durch Anwendungen und auf Speichergeräten vertrauliche Daten versenden, einsehen und drucken: Schützen Sie E-Mail und Webmail, Peer-to-Peer (P2P)-Anwendungen, Instant Messenger, Skype, HTTP, HTTPS, FTP, Wi-Fi, USB, CD, DVD, Drucker, Faxgeräte und externe Speichermedien.
- Verhindern Sie den 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 legitime alltägliche Aktivitäten zu beeinträchtigen

Unternehmensgerechte Geräteverschlüsselung

- Automatische Verschlüsselung ganzer Geräte ohne Zutun der Anwender und ohne Anwenderschulungen durchführen oder Einbußen bei den Systemressourcen hinnehmen 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 Datei- und Ordnerschlüsselung

- 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 – oder sogar als E-Mail-Anhänge - gespeichert werden

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 Auditfunktionen

- Weisen Sie mit umfassenden Auditfunktionen nach, dass Geräte verschlüsselt sind
- Protokollieren Sie Datenübertragungen zur Aufzeichnung von Informationen wie Absender, Empfänger, Zeitstempel, Datenspuren, Datum und Uhrzeit der letzten erfolgreichen Anmeldung, Datum und Uhrzeit des letzten empfangenen Updates sowie der Angabe, ob die Verschlüsselung erfolgreich war oder nicht

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

