



# McAfee® Endpoint Encryption

(ehemals SafeBoot® Encryption)

## Schützen Sie Daten auf PCs, Laptops, Tablet-PCs und PDAs

Der Schutz von Daten gilt bei den CISOs zurzeit als höchste Priorität.<sup>1</sup> McAfee® Endpoint Encryption bietet eine skalierbare, unternehmensweite Sicherheitslösung mit starker Verschlüsselung und strenger Zugangskontrolle, um unbefugten Zugriff auf Daten zu verhindern, die auf Desktops, Laptops und Tablet-PCs sowie auf Smartphones and PDAs gespeichert sind.

### HAUPTVORTEILE

#### Starke Verschlüsselung und strenge Zugangskontrolle

- Schutz vor unbefugtem Zugang und Gefährdung von Daten durch starke Geräteverschlüsselung und strenge Pre-Boot-Authentifizierung
- Transparente Verschlüsselung im laufenden Betrieb, kein Zutun des Anwenders und keine Schulung erforderlich
- Sicherstellung, dass Dateien und Ordner unabhängig vom Speicherort oder Übertragungsziel stets verschlüsselt bleiben

#### Einhaltung betriebsinterner und externer Sicherheitsbestimmungen

- Durchsetzung unternehmensweiter obligatorischer Sicherheitsrichtlinien
- Nachweis der Einhaltung von Datenschutzgesetzen
- Kontrolle, auf welche Anwendungen Benutzer zugreifen dürfen

#### Einfache, zentrale Verwaltung und niedrigere Gesamtbetriebskosten

- Zugriff auf umfassende, zentrale Verwaltungsfunktionen
- Synchronisierung und Integration der Lösung mit Active Directory, Novell, LDAP und PKI
- Mehr Bedienkomfort durch Single-Sign-On und Unterstützung gängiger SmartCards und Tokens
- Unterstützung aller gängigen Sprachen, Tastaturbelegungen und Windows-Betriebssysteme

#### Schützen Sie Ihre Ressourcen und Ihre Marke

Der Verlust vertraulicher Daten, darunter Kundendaten, Personalakten, geistiges Eigentum und Geschäftsdokumente, ist mittlerweile ein allgegenwärtiges Problem für Unternehmen in aller Welt. In einer 2007 durchgeführten Studie des Ponemon Institute gaben 85 Prozent der befragten Unternehmen an, es sei bei ihnen bereits zu einem Datensicherheitsverstoß gekommen.<sup>2</sup> Ebenfalls konnte das Ponemon Institute berichten, dass die durchschnittlichen Folgekosten eines solchen Verstoßes sich auf 6,3 Millionen Dollar belaufen.<sup>3</sup>

#### Erreichen Sie bestmögliche Datensicherheit durch die Verschlüsselung ganzer Festplatten

Der Schutz von Datenbeständen ist heutzutage eine der wichtigsten Aufgaben für Unternehmen. Schützen Sie die unverzichtbaren Daten Ihres Unternehmens mit McAfee Endpoint Encryption. Bei dieser Lösung kommen eine strenge Zugangskontrolle mit Anwender-Authentifizierung noch vor dem Hochfahren des Betriebssystems (Pre-Boot-Authentifizierung) und staatlich zertifizierte Verschlüsselungsalgorithmen zum Schutz von Daten auf Endgeräten wie Desktops, Laptops, Tablet-PCs, Smartphones und PDAs zum Einsatz. Ver- und Entschlüsselung sind für den Anwender transparent, finden bei laufendem Betrieb statt und haben so gut wie keinen Leistungsverlust zur Folge. McAfee Endpoint Encryption integriert sich nahtlos in bestehende Unternehmenssysteme und bietet hohe Effizienz im Betrieb, sodass niedrige Gesamtbetriebskosten garantiert sind.

#### Schützen Sie Dateien und Ordner, wo immer sie sich befinden

Bestimmen Sie, welche Dateien oder Ordner verschlüsselt werden. Mit McAfee Endpoint Encryption können Administratoren die Verschlüsselung der Inhalte bestimmter Ordner sowie von Dateien aus bestimmten Anwendungen oder eines bestimmten Dateityps festlegen. Anwendergruppen erhalten selektive Zugriffsrechte auf bestimmte Dateien und Ordner und können diese über das gesamte Netzwerk hinweg sicher gemeinsam nutzen.

Egal, wo Dateien gespeichert sind oder wohin sie übertragen werden, die Daten bleiben dank der Persistent Encryption Technology™ stets verschlüsselt. Wenn ein unbefugter Anwender versucht, eine Datei, die auf einem Firmenlaptop einsehbar ist, auf einem nicht genehmigten Gerät zu speichern, so erhält er nur eine verschlüsselte und damit unlesbare Datei.

#### Erlangen Sie Richtlinieneinhaltung und niedrigere Gesamtbetriebskosten

Nutzen Sie ein umfassendes, komplett über eine zentrale Konsole verwaltetes Spektrum von Sicherheits- und Verschlüsselungslösungen, um Datenverlusten vorzubeugen, wozu auch immer Ihre Daten gehen, und gesetzliche Bestimmungen einzuhalten. Die zentralen Verwaltungsfunktionen von McAfee Endpoint Encryption umfassen unter anderem Administration, zentrale Bereitstellung, Remote-Updates, Auditing, Verwaltung von obligatorischen Sicherheitsrichtlinien, ein Scripting-Tool, Hot-Revocation, Passwort-Wiederherstellung, Synchronisierung usw. Mit umfassenden Auditing-Funktionen lässt sich beweisen, dass ein Gerät zum Zeitpunkt seines Verlustes oder Diebstahls verschlüsselt war, sodass auch der Nachweis für die Richtlinieneinhaltung erbracht ist. Obligatorische Sicherheitsrichtlinien können von Administratoren transparent durchgesetzt werden. McAfee Endpoint Encryption unterstützt auch Single-Sign-On und die sichere Offline-Wiederherstellung von Benutzerpasswörtern.

<sup>1</sup> Merrill Lynch-Umfrage unter CISOs von 2007

<sup>2</sup> 2007 durchgeführte Studie des Ponemon Institute zu betriebswirtschaftlichen Folgen von Datenlecks (Business Impact of Data Breach)

<sup>3</sup> 2007 durchgeführte Studie des Ponemon Institute zu Kosten von Datenverlusten (Cost of a Data Breach Study)

## SYSTEMANFORDERUNGEN

### Desktop-, Laptop- und Tablet-PC-Endgeräte

#### Betriebssysteme

- Microsoft® Windows Vista (alle 32- und 64-bit-Versionen)
- Microsoft® Windows XP
- Microsoft® Windows 2000
- Microsoft® Windows Server 2003

#### Hardware-Anforderungen

- Prozessor: Pentium-kompatibel
- RAM: min. 128 MB
- Festplattenspeicher: 5-35 MB, je nach Lokalisierung und Geräteanzahl
- Netzwerkanschluss: TCP/IP für Remote-Zugriff

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

### Zentrale Verwaltung

#### Betriebssysteme

- Microsoft® Windows 2000
- Microsoft® Windows XP
- Microsoft® Windows Server 2003

#### Hardware-Anforderungen

- RAM: 128 MB: 512 MB empfohlen
- Festplattenspeicher: 200 MB
- Prozessor: Pentium-kompatibel

### Starke Verschlüsselung und strenge Zugangskontrolle

Schützen Sie mit der Verschlüsselung ganzer Festplatten Ihre Desktops, Laptops, Tablet-PCs, Smartphones und PDAs sowie die Daten auf deren Festplatten vor unbefugtem Zugriff oder unbefugter Verwendung.

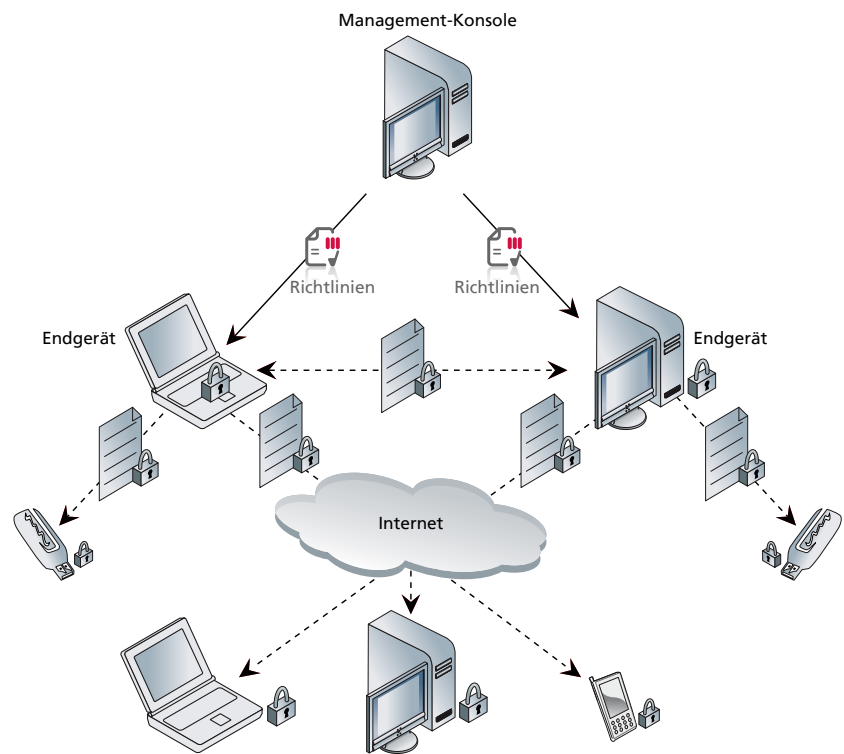
- Überprüfen Sie zusätzlich zur herkömmlichen Passwort-Authentifizierung sowohl den Anwender als auch das Gerät noch vor dem Hochfahren des PCs anhand einer Zwei-Faktor-Pre-Boot-Authentifizierung.
- Erhalten Sie unerreichten Schutz durch eine branchenweit führende, mehrfach ausgezeichnete Verschlüsselung mit Algorithmen wie AES-256 und RC5-1024.
- Verschlüsseln Sie Geräte transparent, ohne Auswirkungen auf den Tagesbetrieb und ohne Anwenderschulungen.
- Stellen Sie mit Persistent Encryption Technology™ sicher, dass Dateien und Ordner unabhängig von ihrem Speicherort stets verschlüsselt sind.

### Erfüllen Sie betriebsinterne und externe Sicherheitsanforderungen

- Weisen Sie eine umfassende und lückenlose Protokollierung nach und erhalten Sie Schutz im Sinne der Safe Harbor-Datenschutzrichtlinie, so dass der Verlust eines Laptops oder USB-Laufwerks keinen meldepflichtigen Verstoß darstellt.
- Legen Sie umfassende obligatorische Sicherheitsrichtlinien fest und setzen Sie sie durch.
- Bestimmen Sie, welche speziellen Dateitypen oder Ordner ohne Zutun des Endanwenders verschlüsselt werden.
- Ziehen Sie den optimalen Nutzen aus der Zertifizierung nach FIPS 140-2 und Common Criteria EAL4.

### Einfache, zentrale Verwaltung und niedrigere Gesamtbetriebskosten

- Beugen Sie Datenverlusten umfassend vor und nutzen Sie ein komplettes Spektrum von Sicherheits- und Verschlüsselungslösungen, die alle von einer zentralen Konsole aus verwaltet werden.
- Beweisen Sie die Einhaltung von Datenschutzbestimmungen und schützen Sie Ihre Ressourcen und Ihre Marke, sichern Sie sich die Treue Ihrer Kunden und einen Wettbewerbsvorteil.
- Sorgen Sie mühelos für die unternehmensweite Bereitstellung und Verwaltung von Richtlinien und sparen Sie Zeit und Geld.
- Stellen Sie Passwörter und Tokens sicher per Fernzugriff wieder her. Das Passwort eines Anwenders kann nach einer Sprachverifizierung und -authentifizierung zurückgesetzt werden, so dass weniger Zeit- und Arbeitsaufwand für den Helpdesk anfällt.



### McAfee Endpoint Encryption

Weitere Informationen zum Thema Datenschutz finden Sie unter [www.mcafee.com/data\\_protection](http://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](http://www.mcafee.de)

