



McAfee® Device Control

Verhindern Sie die unbefugte Verwendung von externen Speichergeräten in Ihrem Netzwerk

So nützlich USB-Laufwerke, MP3-Player, DVDs und andere Wechseldatenträger auch sind – für Ihr Unternehmen stellen sie eine echte Bedrohung dar. Gerade weil diese Datenträger bei äußerst kompakten Abmessungen eine enorme Speicherkapazität bieten, kann es nur zu leicht geschehen, dass mit ihrer Hilfe vertrauliche Kundendaten und geistiges Eigentum zunächst direkt durch den Vordereingang aus Ihrem Unternehmen gelangen und dann durch Verlust oder Diebstahl in die falschen Hände geraten.

In einer von McAfee®, Inc. durchgeführten Umfrage gaben mehr als die Hälfte der Befragten (etwa 55 Prozent) an, jede Woche auf tragbaren Geräten vertrauliche Dokumente von ihrem Arbeitsplatz mitzunehmen.¹ Aber wie können Sie wissen, wer was auf welchem Gerätetyp speichert? Und selbst wenn die Mitarbeiter Ihre Genehmigung zur Verwendung der Daten haben: Wie können Sie sicher sein, dass sie sorgfältig genug damit umgehen?

HAUPTVORTEILE

Unerreichter Schutz

- Schutz vor Datenverlust durch die unbefugte Verwendung von Wechseldatenträgern

Umfassendes Gerätemanagement

- Einrichtung detaillierter hardware- und inhaltsabhängiger Filterung, Überwachung und Sperrung von Kopien vertraulicher Daten auf beliebige Wechseldatenträger
- Freigabe zur sicheren Verwendung von Wechseldatenträgern – kein "Block All"-Ansatz mit Beeinträchtigung der Produktivität nötig

Zentrale Verwaltung mit ePO

- Optimale Nutzung Ihrer McAfee Sicherheitsrisikomanagement-Plattform zum Schutz vor Datenverlusten durch Wechseldatenträger
- Zentrale Bereitstellung und Verwaltung von Sicherheitsrichtlinien zum Schutz vor dem Verlust vertraulicher Daten durch Wechseldatenträger

Komplette Übersicht

- Nachweis von Maßnahmen zur Einhaltung interner und gesetzlicher Richtlinien gegenüber Auditoren, Vorstandsmitgliedern und anderen Interessengruppen

Wenden Sie steigende Risikokosten ab

Heutzutage ist Datenverlust eines der häufigsten, schwerwiegendsten und kostspieligsten Probleme für Unternehmen. Tatsächlich sind über 75 Prozent der Fortune-1000-Unternehmen bereits Opfer von versehentlichem oder böswilligem Datenverlust geworden. Und die Kosten sind schwindelerregend. 2007 betrug die durchschnittlichen Folgekosten für ein Unternehmen, das einen Datenschutzverstoß hinnehmen musste, 6,3 Millionen Dollar.²

Überwachen und steuern Sie Datenkopien auf tragbaren Geräten und Speichermedien

Mit McAfee® Device Control können Sie verhindern, dass wichtige Daten auf Wechseldatenträgern wie USB-Laufwerken, iPods, Bluetooth-Geräten sowie beschreibbaren CDs und DVDs Ihr Unternehmen verlassen. Es gibt Ihnen genau die Hilfsmittel an die Hand, die Sie benötigen, um Datenübertragungen von allen Desktops und Laptops zu überwachen und zu steuern – egal, wo sich Anwender und Daten gerade befinden, und selbst wenn sie nicht mit dem Firmennetz verbunden sind.

Mit Device Control erhalten Sie eine fein abgestufte Kontrolle über Ihre sensiblen Daten. Sie können festlegen, welche Geräte verwendet werden dürfen und welche nicht. Sie können bestimmen, welche Daten auf zugelassene Geräte kopiert werden dürfen und welche nicht. Und sie können Anwendern das Kopieren von Daten aus bestimmten Quellen oder Anwendungen verweigern, etwa von einem Dateiserver, auf dem vertrauliche Unternehmensdaten lagern, oder aus einem Buchhaltungsprogramm, mit dem vertrauliche Berichte erzeugt werden.

Setzen Sie detaillierte Geräte- und Datenrichtlinien automatisch durch

Eine zentrale Kontrollmöglichkeit über Ihre Informationsbestände zu erhalten, ist ganz einfach. Mit dem McAfee ePolicy Orchestrator® (ePO™) können Sie den McAfee Device Control-Agenten auf alle verwalteten Desktops und Laptops aufspielen. Dann können Sie ganz genau festlegen, welche Inhalte auf welche Wechseldatenträger kopiert werden dürfen und welche nicht. Die restliche Arbeit nimmt Ihnen Device Control ab, indem es automatisch den Umgang mit Daten und Geräten überwacht und jeden Versuch Geräte zu verwenden oder Daten zu übertragen, die nicht Ihren Richtlinien entsprechen, zu unterbinden – sogar bei veränderten, kopierten, eingefügten, komprimierten oder verschlüsselten Daten. Legitime Unternehmensabläufe dagegen werden durch Device Control nicht beeinträchtigt oder unterbrochen.

Weisen Sie jederzeit die Einhaltung von Bestimmungen und Vorgaben nach

McAfee Device Control gibt Ihnen einen vollständigen Überblick und die komplette Kontrolle über die Übertragung vertraulicher Informationen auf Wechseldatenträger und -medien. Dank der Integration in ePO können sie mühelos wichtige Daten zur Verwendung von Inhalten sammeln, wie zum Beispiel Gerät, Zeitstempel und Datenspuren. Ein einfacher Mausklick ermöglicht Event-Monitoring in Echtzeit und die Ausgabe detaillierter Berichte, die gegenüber Auditoren, Vorstandsmitgliedern und anderen Interessengruppen wirksame Maßnahmen zur Einhaltung unternehmensinterner und gesetzlicher Richtlinien nachweisen.

¹ McAfee. The Threats Within Volume II: Data Loss Disaster. (Zweite Studie zum Risiko eines Datenverlustes durch betriebsinterne Sicherheitslücken.) Februar 2007.

² 2007 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

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

Device Control Endpoint

Betriebssysteme

- Microsoft® Windows XP Professional SP1 oder höher
- Microsoft® Windows 2000 SP4 oder höher

Hardware-Anforderungen

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

Funktionen

Unerreichter Datenschutz

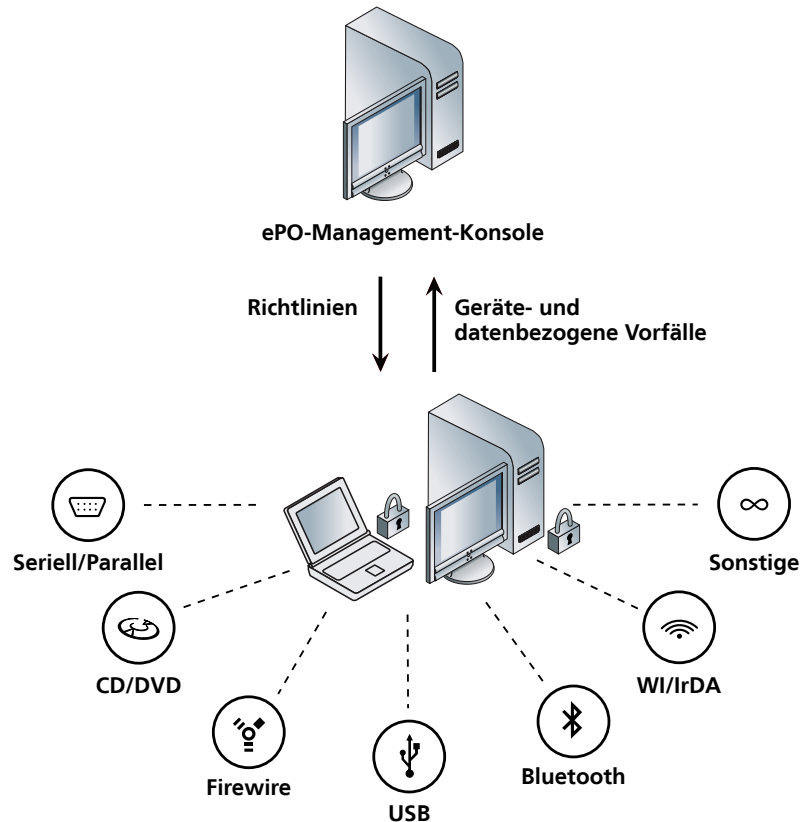
- Legen Sie fest, wie Anwender Daten auf USB-Laufwerke, iPods, beschreibbare CDs und DVDs, Disketten, Bluetooth- und Infrarot-(IrDA-)Geräte, bildgebende Geräte, serielle und parallele Schnittstellen usw. kopieren dürfen
- Schützen Sie alle Daten, Formate und Ableitungen, selbst wenn diese verändert, kopiert, eingefügt, komprimiert oder verschlüsselt wurden
- Verhindern Sie Datenverluste unabhängig vom Aufenthaltsort der Anwender und ohne Beeinträchtigung der normalen Arbeitsabläufe

Zentrale Verwaltung durch McAfee ePO

- Nutzen Sie die schnelle und einfache Konfiguration, Bereitstellung und Aktualisierung von Richtlinien und Agenten in Ihrer gesamten Netzwerkumgebung über eine zentrale Management-Konsole
- Legen Sie Geräte- und Datenrichtlinien nach Anwender, Gruppe oder Abteilung fest
- Legen Sie in Abhängigkeit von jedem beliebigen Windows-Geräteparameter wie Produkt- und Hersteller-ID, Seriennummer, Geräteklasse, Geräteklasse, Geräteklasse usw. fest, welche Geräte verwendet werden dürfen und welche nicht
- Bestimmen Sie, welche Inhalte auf zugelassene Geräte kopiert werden dürfen und welche nicht

Komplette Übersicht und Kontrolle auf Abruf

- Unterstützen Sie Auditierung und Richtlinieneinhaltung durch detaillierte Protokolle auf Anwender- und Geräteebene
- Sammeln Sie zur schnellen und angemessenen Reaktion, Untersuchung und Überprüfung von Vorfällen genaue Angaben zu Gerät, Zeitstempel, Datenspuren usw.



Über McAfee Device Control wird festgelegt, welche Geräte verwendet und welche Daten kopiert werden dürfen. Weitere Informationen zum Thema Datenschutz finden Sie 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-ins-001-0108