

# McAfee Host Data Loss Prevention

Geraten Sie nicht wegen eines Datenverlustes in die Schlagzeilen

Verlieren Sie Daten, ohne es zu wissen? Ihre Kundeninformationen, geistiges Eigentum, Finanzdaten und Personalakten könnten in diesem Moment aus Ihrem Unternehmen gelangen. Und die Täter sind nicht unbedingt Hacker – es können auch Ihre eigenen Mitarbeiter sein. Versehentliche oder böswillig herbeigeführte Datenverluste können sich über gängige Medien wie E-Mails, Internetveröffentlichungen, USB-Laufwerke oder Drucker ereignen, und die dadurch verursachten Kosten können in die Millionen gehen.

## Hauptvorteile

### Einzigartiger Schutz

- Schutz vor Datenverlust, wo immer Ihre Daten sich befinden: am Arbeitsplatz, zu Hause und unterwegs

### Umfassendes Geräte-Management

- Festlegung detaillierter, inhaltsabhängiger Richtlinien zur Filterung, Überwachung und Sperrung vertraulicher Daten auf beliebigen externen Speichermedien

### Mehrstufiger Schutz

- Stellen Sie sicher, dass Ihre Daten auf allen Endgeräten geschützt sind, und zwar unabhängig von Betriebssystem oder Gerätetyp

### Zentrale Verwaltung mit ePO

- Optimale Nutzung Ihrer McAfee Sicherheitsrisiko-Management-Architektur zur Vermeidung von Datenverlusten

### Vollständige Transparenz

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

## Schützen Sie sich vor Datenverlust, bevor er sich ereignet

Tag für Tag werden Unternehmen wie Ihres Opfer erheblicher Datenverluste durch versehentliches oder böswillig herbeigeführtes Durchsickern von Information. Laut einer aktuellen Studie sind über 75 Prozent der Fortune-1000-Unternehmen bereits Opfer von Datenverlust geworden. Laut einer aktuellen Studie verwenden mehr als 55 Prozent der Mitarbeiter tragbare Geräte, um jede Woche vertrauliche Daten vom Arbeitsplatz mitzunehmen.<sup>1</sup> Die Folgekosten solcher Datenverluste und deren Behebung für Unternehmen sind extrem hoch. 2008 lagen sie im Durchschnitt bei 6,65 Millionen US-Dollar.<sup>2</sup>

Was wäre, wenn Sie Datenverluste einfach und wirkungsvoll verhindern könnten? Was wäre, wenn Sie gleichzeitig zur Einhaltung von Branchenrichtlinien und gesetzlichen Bestimmungen beitragen könnten? Jetzt können Sie das – mit einer Lösung zur Überwachung, Prüfung und Steuerung des Umgangs der Anwender mit Ihren vertraulichen Daten.

## Schutz und Richtlinieneinhaltung

Erhalten Sie vollständige Übersicht und Kontrolle über den Transfer Ihrer wichtigsten Daten mit McAfee® Host Data Loss Prevention (Host DLP). Überwachen Sie Ihre vertraulichen Daten und verhindern Sie Datenverluste am Arbeitsplatz, zu Hause und unterwegs. Host DLP schützt Ihr Unternehmen vor den Risiken finanzieller Verluste, Image-Schäden, Kundenverluste, Wettbewerbsnachteilen und Richtlinienverstößen.

Mit Host DLP können Sie Vorgänge schnell und einfach in Echtzeit überwachen, zentral verwaltete Sicherheitsstrategien anwenden, um die Nutzung und Übertragung vertraulicher Daten durch Ihre Mitarbeiter zu regulieren und zu beschränken. Des Weiteren können Sie detaillierte forensische Berichte erstellen, ohne den laufenden Geschäftsbetrieb zu beeinträchtigen.

Schützen Sie Ihr Unternehmen vor drohenden Datenverlusten innerhalb des Betriebes, etwa durch E-Mail, Instant Messenger, gebrannte CDs, Veröffentlichungen im Internet, Kopien auf USB-Laufwerken und Ausdrucken. Dazu erhalten Sie Schutz vor dem Verlust vertraulicher Daten durch Trojaner, Würmer oder Filesharing-Anwendungen, die ohne das Wissen Ihrer Mitarbeiter deren Zugangsdaten übernehmen.

## Schutz ohne Störung

Schützen Sie sich vor Datenverlusten, ohne normale Geschäftsabläufe zu stören, selbst wenn Daten verändert, kopiert, eingefügt, komprimiert oder verschlüsselt werden. Schützen Sie Inhalte in mehr als 390 Dateitypen. Einzigartige Fingerprinting-Algorithmen und die Möglichkeit, Inhalte durch Tagging zu kategorisieren (nach Speicherort, Anwendung, Dateityp, Standardausdrücken, Schlüsselwörtern usw.), sorgen für breitgefächerten und tiefgreifenden Datenschutz und gewährleisten, dass die Daten Ihres Unternehmens sicher sind.

## Vereinfachtes Compliance-Management

Die einfache Verwaltung mit McAfee ePolicy Orchestrator® (McAfee ePO™) ermöglicht Event-Monitoring und das Festhalten von Ereignisdetails zum Nachweis der Einhaltung firmeninterner und gesetzlicher Vorschriften gegenüber Auditoren, Vorstandsmitgliedern und anderen Interessengruppen. Dank der Integration von Host DLP in ePO können Sie mühelos wichtige Daten zur Verwendung von Inhalten sammeln, wie zum Beispiel Gerät, Zeitstempel und Datenspuren. ePO ermöglicht mit nur einem Klick Event-Monitoring und detaillierte Berichte zum Nachweis der Einhaltung firmeninterner und gesetzlicher Richtlinien gegenüber Auditoren, Vorstandsmitgliedern und anderen Interessengruppen.

## Ihr Gewinn: Einzigartiger Datenschutz

Sie erhalten die volle Kontrolle und Übersicht über alle Daten, die Ihre Endgeräte verlassen, um Verlusten – und den negativen Schlagzeilen – von vornherein vorzubeugen.

1. Illuminas 2007, Threats Within Volume II Data Loss Disaster (Zweite Studie zum Risiko eines Datenverlustes durch betriebsinterne Sicherheitslücken)

2. 2008 durchgeführte Studie zu Kosten von Datenverlusten des Ponemon Institute (Cost of Data Breach Study)

**Systemanforderungen**

**ePO-Server**

- Betriebssysteme
- Microsoft® Server 2003 SP1, 2003 R2

**Desktop- und Laptop-Endgeräte**

- Betriebssysteme
- Microsoft Windows® XP Professional ab SP1
- Microsoft Windows 2000 ab SP4

**Hardware-Anforderungen**

- Prozessor: Pentium III 1 GHz oder höher
- RAM: 512 MB (empfohlen)
- Freier Festplattenspeicher: mindestens 200 MB
- Netzwerkanschluss: TCP/IP für Remote-Zugriff

Host DLP ist Teil einer Gesamtlösung für Datenschutz. McAfee Total Protection™ for Data ist eine Kombination von Host DLP und McAfee Endpoint Encryption und bietet so eine noch umfassendere Datenschutzlösung.

**Funktionen**

**Einzigartiger Schutz**

- Sie erhalten vollständige Kontrolle darüber, wie die Anwender über das Netzwerk, durch Anwendungen und auf Speichergeräten vertrauliche Daten versenden, einsehen und drucken. 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.
- DLP bietet die folgenden Optionen für die Richtliniendurchsetzung:
  - » Überwachung – Datenübertragung zulassen
  - » Schutz – Datenübertragung sperren
  - » Warnung – Administrator und Endanwender benachrichtigen
  - » Verschlüsselung – Verschlüsselung vor Versenden sicherstellen\*
  - » Quarantäne – auf Genehmigung warten\*

\*Enthalten in der McAfee Data Loss Prevention-Appliance

**Umfassendes Geräte-Management**

- Kontrollieren und sperren Sie Kopien vertraulicher Daten auf USB-Geräten, Flash-Laufwerken, iPods und anderen externen Speichermedien.
- Legen Sie verwendbare Geräte fest und teilen Sie nach jedem beliebigen Windows-basierten

Geräteparameter wie Produkt-ID, Hersteller-ID, Seriennummer, Geräteklasse, Gerätenamen usw. in Kategorien ein

**Mehrstufiger Schutz für Endgeräte**

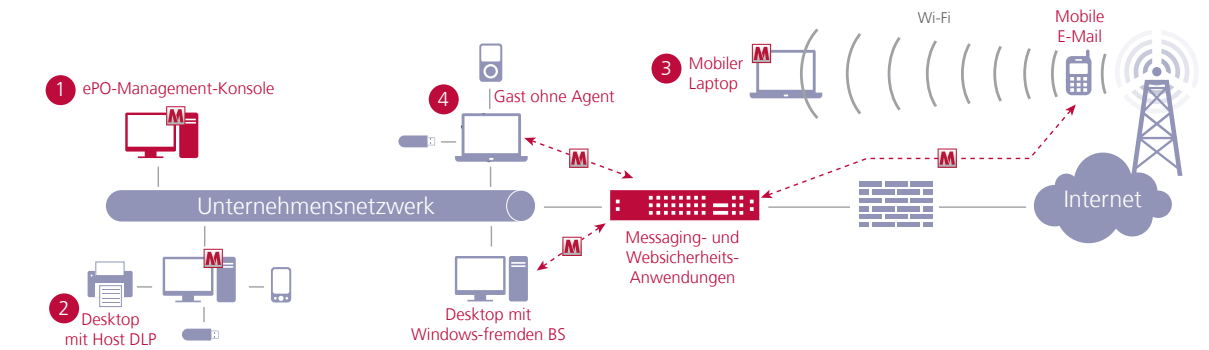
- Host-basierter Schutz verhindert Datenverluste über Endgeräte durch Überwachung und Sperrung des riskanten Umgangs von Anwendern mit Ihren vertraulichsten Daten
- In Kombination mit Endpoint Encryption gewährleistet Host DLP einen umfassenden, mehrstufigen Ansatz zum Schutz vor Datenverlust

**Zentrale Verwaltung mit ePO**

- Erhalten Sie Zugang zu zentralen DLP-Richtlinien und Event-Monitoring über die ePO-Management-Konsole
- Nutzen Sie ePO für zentrale Richtlinienverwaltung und Ereignisüberwachung
- Nutzen Sie ePO für Bereitstellung und Aktualisierung von Agenten
- Die Integration mit ePO 4.0 ermöglicht fortschrittliches, Web-basiertes Management und zusätzliche Reporting/Audit-Funktionen

**Komplette Übersicht auf Abruf**

- Nutzen Sie das umfassende Funktionsspektrum von Host DLP für Überwachung und Ereignisberichte, um alle für exakte Analysen, Untersuchungen und Audits, zur Schadensbegrenzung und Risikobewertung erforderlichen Daten wie Absender, Empfänger, Zeitstempel und Datenspuren zu sammeln



- 1 ePO-Management-Konsole** - Zentrale Richtlinienverwaltung, Auditing, Berichterstattung und Softwareverteilung. Gewährleistet, dass Ihre Sicherheitsrichtlinien exakt auf Ihre Geschäftsabläufe und -tätigkeiten zugeschnitten sind.
- 2 Host DLP und Endpoint Encryption** – Überwachung, Berichterstattung, Kontrolle und Schutz vor Anwenderverhalten, das Ihre Daten gefährden könnte. Starke, FIPS-zertifizierte Verschlüsselung des gesamten Laufwerks oder einzelner Dateien oder Ordner zum Schutz der Datenintegrität bei Verlust oder Diebstahl.
- 3 Endpoint Encryption for Mobile** – Richtet auf tragbaren Geräten verschlüsselten, geschützten Speicherplatz für vertrauliche Daten ein. Schützt die Integrität und Vertraulichkeit dieser Daten bei Verlust oder Diebstahl des Geräts.
- 4 Device Control und Endpoint Encryption** – Kontrolliert den Umgang von Anwendern mit externen Mediengeräten wie iPods und USB-Sticks zum Schutz vor Verlust vertraulicher Daten. Durch starke Verschlüsselung ganzer Laufwerke ist gewährleistet, dass der Laptop bei Verlust oder Diebstahl unbrauchbar wird.

