

# McAfee Data Loss Prevention Monitor

## Schutz wichtiger Daten

Der Schutz von Kunden- und persönlichen Mitarbeiterdaten, einschließlich Kreditkartendaten und Steueridentifikationsnummern sowie anderer persönlicher Daten, wird derzeit viel diskutiert. Unbeabsichtigte Datenkompromittierungen durch Fehlverhalten von Angestellten, verloren gegangene Laptops und verlegte USB-Geräte stellen für fast alle Unternehmen eine ernsthafte Sicherheitsbedrohung dar. Die Situation wird dadurch erschwert, dass Daten auch dann kompromittiert werden oder in den falschen Händen landen können, wenn sie über Web-Anwendungen wie Google Gmail, Yahoo! Mail, Sofortnachrichten und Facebook übertragen werden. McAfee® Data Loss Prevention Monitor (McAfee DLP Monitor) ist eine Hochleistungslösung zum Schutz vor Datenkompromittierungen, die die gesamte Internetkommunikation analysieren und feststellen kann, ob Informationen unerwünschte Wege gehen. Die Lösung unterstützt Sie dabei, die Belastung des Sicherheitsteams zu minimieren, die Compliance-Vorgaben zu erfüllen und den Schutz von geistigem Eigentum und anderen wichtigen Ressourcen zu gewährleisten.

### Bewegliche Daten überwachen, verfolgen und Berichte erstellen

Unabhängig von Ihrer Branche benötigen Sie einen genauen Überblick über alle vertraulichen Informationen, die – in welcher Form auch immer – über Anwendungen, Protokolle oder Ports übertragen werden.

Mit McAfee DLP Monitor können Sie den Datenverkehr in Ihrem gesamten Netzwerk in Echtzeit erfassen, nachverfolgen und darüber Berichte erstellen, so dass Sie über die Datenströme zwischen den Anwendern

und anderen Unternehmen genau im Bilde sind. McAfee DLP Monitor ist eine leistungsfähige, speziell entwickelte Appliance, die mehr als 300 Inhaltstypen, die über beliebige Ports oder Protokolle übertragen werden, eindeutig erkennt. Mit dieser Lösung können Datenbedrohungen erkannt und Maßnahmen zum Schutz des Unternehmens vor Datenverlusten ergriffen werden. Zusätzlich kann McAfee DLP Monitor zur Mitarbeiterschulung über richtlinienkonformes Verhalten beitragen, indem Ihre Benutzer benachrichtigt werden, sobald sie Datenschutzrichtlinien verletzen.

## Hauptvorteile

- Erkennung und Schutz vertraulicher Daten
  - Schnelles Auffinden vertraulicher Informationen dank einer intuitiven Suchmaschine
  - Durchführung forensischer Analysen zur Korrelation aktueller und vergangener Risikoereignisse, Erkennung von Risikotrends und Identitätsbedrohungen
  - Sofortige Regelerstellung zur Abwendung zukünftiger Gefahren
- Vollständig in die Software McAfee® ePolicy Orchestrator® (McAfee ePO™) integriert
- Verwaltung vollständig über McAfee ePO möglich – für gemeinsame Richtlinienverwendung, Zwischenfall- und Fall-Management über McAfee DLP Endpoint sowie Erstellung und Anpassung komplexer Regeln
  - Erkennung von mehr als 300 Inhaltstypen an allen Ports und in allen Anwendungen
  - Analyse des Netzwerkverkehrs unabhängig vom Port
  - Erweiterung zur Unterstützung von mehreren Hunderttausend Verbindungen gleichzeitig

### Informationen in Echtzeit scannen und analysieren

McAfee DLP Monitor ist in das Netzwerk integriert und scannt sowie analysiert den Netzwerkverkehr in Echtzeit mittels eines SPAN- oder Tap-Ports. Mit mehr als 150 vordefinierten Regeln, die von Richtlinien-einhaltung bis zur zulässigen Verwendung geistigen Eigentums reichen, kann McAfee DLP Monitor sogar geringfügige Abweichungen in Dokumentteilen feststellen und so Unregelmäßigkeiten im Netzwerkverkehr unabhängig von ihrem Ausmaß erkennen.

### Risiken aufdecken, die Ihnen bisher nicht bewusst waren

Da McAfee DLP Monitor nicht nur die von den Echtzeitregeln erfassten Informationen, sondern den gesamten Netzwerkverkehr detailliert klassifiziert, indexiert und speichert, können Sie die Verlaufsdaten unmittelbar nutzen, um vertrauliche Daten, die Art ihrer Verwendung sowie die sie verwendende Person zu erkennen und den Übertragungsweg nachzuverfolgen. Zusätzlich können Sie Informationen genauer untersuchen und die zugehörigen Verlaufsdaten überprüfen, um Risikoereignisse und die Gefährdungssituationen zu erkennen, die bis dahin unbemerkt geblieben sind. Bei gemeinsamer Nutzung mit McAfee DLP Discover können Sie außerdem erkennen, wo Daten in Ihrem Netzwerk gespeichert sind und wem diese gehören.

### Fundierte Entscheidungen treffen

Nachdem der Netzwerkverkehr gescannt, analysiert und mithilfe der Klassifizierungs-Engine klassifiziert wurde, speichert McAfee DLP Monitor alle wichtigen Informationen in einer eigenen Datenbank. Mithilfe einer intuitiven Suchmaske können Sie umfassende Berichte über Ihre Daten, die Personen, die sie versenden, sowie die Übertragungswege und -methoden ansehen und so feststellen, welche Informationen wo und von wem preisgegeben werden. Mit diesem Wissen können Sie eine Reihe von Maßnahmen anwenden, um diese Bedrohungen abzuwehren, die Richtlinienkonformität sicherzustellen und vertrauliche Daten zu schützen.

### Spezifikationen

---

**Systemdurchsatz:** Inhaltsklassifizierung mit bis zu 200 Mbit/s, ohne Probenentnahme

**Netzwerkintegration:** Passive Integration in das Netzwerk, entweder mittels SPAN-Port oder über einen physikalischen Inline-Netzwerk-Tap (optional)

**Unterstützung der Klassifizierung von über 300 Inhaltstypen, wie:**

- Microsoft Office-Dokumente
- Multimediadateien
- P2P-Dateien
- Quell-Code
- Design-Dateien
- Archive
- Verschlüsselte Dateien

### Alle Datentypen klassifizieren

McAfee DLP Monitor ermöglicht Ihrem Unternehmen, verschiedenste vertrauliche Daten zu scannen – von allgemeinen, in einem festgelegten Format vorliegenden Daten bis hin zu komplexem und hoch variablem geistigen Eigentum. Durch die Kombination dieser Objektklassifizierungsverfahren schafft McAfee DLP Monitor eine äußerst genaue, detaillierte Klassifizierungs-Engine, die vertrauliche Informationen filtert und verborgene bzw. unbekannte Risiken aufdeckt.

Zu den Objektklassifizierungsverfahren zählen:

- **Mehrstufige Klassifizierung:** Fasst sowohl Kontextdaten als auch Inhalte in einem hierarchischen Format zusammen.
- **Dokumentenregistrierung:** Berücksichtigt auch die „biometrischen“ Signaturen der Daten, während sich diese verändern.

- **Grammatische Analyse:** Erkennt grammatische oder syntaktische Strukturen in allen Dokumenttypen, von Texten über Tabellenblätter bis hin zu Quellcodedateien.
- **Statistische Analyse:** Verfolgt, wie häufig eine Signatur, eine grammatische Struktur oder ein „biometrisches“ Muster in einem bestimmten Dokument oder in einer Datei vorhanden ist.
- **Dateiklassifizierung:** Erkennt die Inhalte von Dateien unabhängig von der zugewiesenen Dateinamenerweiterung oder einer Verschlüsselung.

### Formfaktoren und Appliance-Optionen

McAfee DLP Monitor ist als Hardware- bzw. virtuelle Appliance verfügbar. Weitere Details finden Sie im **Datenblatt zur McAfee DLP 6600-Hardware-Appliance**.

### Spezifikationen (Fortsetzung)

#### Unterstützte Protokolle

- Unterstützung von Übertragungen über alle Protokolle oder Ports, die TCP als Transportprotokoll verwenden
- Protokollhandler für HTTP, HTTPS, SMTP, IMAP, POP3, FTP, Telnet, Rlogin, SSH, Webmail, Yahoo! Chat, AOL Chat, MSN Chat, ICY, RTSP, SOCKS, PCAnywhere, RDP, VNC, SMB, Citrix, Skype, IRC, LDAP, DASL, NTLM, Kazaa, BitTorrent, eDonkey, Gnutella, DirectConnect, MP2P, WinMX, Sherlock, eMule und weitere

#### Integrierte Richtlinien

- Zahlreiche integrierte Richtlinien und Regeln für allgemeine Anforderungen, z. B. zum Schutz der Richtlinien-Compliance, des geistigen Eigentums und zur Blockierung unzulässiger Nutzung
- Regeln durch die Nutzung der McAfee-Erfassungsdatenbank vollständig an unternehmensspezifische Anforderungen anpassbar



Ohmstr. 1  
85716 Unterschleißheim  
Deutschland  
+49 (0)89 3707 0  
[www.mcafee.com/de](http://www.mcafee.com/de)

McAfee, das McAfee-Logo, ePolicy Orchestrator und McAfee ePO sind Marken oder eingetragene Marken von McAfee, LLC oder seinen Tochterunternehmen in den USA und anderen Ländern. Alle anderen Namen und Marken sind Eigentum der jeweiligen Besitzer. Copyright © 2017 McAfee, LLC. 3002\_0517  
MAI 2017