

# Typische Anwendungsfälle für McAfee Data Loss Prevention

Im Folgenden sind typische Anwendungsfälle für McAfee® Data Loss Prevention (DLP) zu Ihrer Orientierung dargestellt.

## McAfee Network Data Loss Prevention - Monitor

Anwendungsfall	Beispiel
Kontrolle über nicht autorisierte Prozesse	Überwachung auf Sicherheitslücken bei Instant Messaging und Peer-to-Peer-Übertragungen
Einhaltung gesetzlicher Bestimmungen	Medizinische Angestellte versenden Patientendaten an private Webmail-Konten, um zu Hause damit zu arbeiten
Verschlüsselung	Automatische Verschlüsselung sensibler Daten, die für einen Geschäftspartner oder Kunden bestimmt sind
Regelbasierte Blockierung oder Quarantäne	Zurückhaltung und Überprüfung von E-Mails an Wettbewerber, die Finanzdaten des Unternehmens oder geistiges Eigentum enthalten
Überwachung und/oder Blockierung von SSL-Kanälen	Einsicht in SSL-verschlüsselte Webmail-Übertragungen oder PGP-verschlüsselte E-Mails
Sensibilisierung der Mitarbeiter	Automatische Benachrichtigung der Angestellten und/oder des Managements bei Verstößen gegen die Richtlinien zum Datenschutz und zum Schutz gegen Belästigung
Untersuchung auf unentdeckte Sicherheitslücken	Untersuchung aller Kommunikationskanäle, ob Angestellte Geschäftsgeheimnisse an Wettbewerber weitergeben
Zulässige Nutzung	Sicherstellung, dass keine Bilder oder Materialien zweifelhaften Charakters versendet werden
Identifizierung geistigen Eigentums	Zuverlässige Bestimmung des Speicherorts und Datentyps sensibler Daten

## McAfee Network Data Loss Prevention - Discover

Anwendungsfall	Beispiel
Konformität mit den Richtlinien von GLBA, PCI DSS und HIPAA <sup>1</sup>	Unverschlüsselte Speicherung von CCN-Daten auf Laufwerken
Überprüfung der Anwender	Durchsuchung aller Festplatteninhalte auf dem System eines Angestellten, der nicht jugendfreie Webseiten besucht
eDiscovery	Findung und Indexierung von Inhalten auf Systemen oder Repositories wie Microsoft SharePoint
Datenklassifizierung	Zuverlässige Bestimmung des Speicherorts und Datentyps sensibler Daten
Datenzugriffs-Audit	Suche nach Lohn- oder Angestelltendaten auf Verkaufscomputern
Verlust von Laptops und Backup-Bändern	Abbild der gespeicherten Daten

<sup>1</sup> Gramm-Leach-Bliley Act (GLBA), Payment Card Industry Data Security Standard (PCI DSS) und Health Insurance Portability and Accountability Act (HIPAA)

## McAfee Host Data Loss Prevention

Anwendungsfall	Beispiel
Anwendungsverwaltung von externen Wechseldatenträgern	Verhinderung der Übertragung von sensiblen Daten, geistigen Eigentums oder von Kundendaten auf unsichere externe USB-Datenträger
Blockierung risikoreicher Handlungen in Unternehmensanwendungen	Unterbindung des Kopieren, Einfügen und Drucken sensibler Daten in Unternehmensanwendungen wie Enterprise Resource Planning (ERP) und Customer Relationship Management (CRM)
Sensibilisierung der Mitarbeiter	Angestellte werden in Echtzeit über Verstöße gegen Richtlinien informiert, sobald diese in ihren Systemen auftreten und ggf. aufgefordert, diese zu rechtfertigen
Datenschutz im Offline-Status	Verhinderung, dass ein mobiler Angestellter von einem Cafe aus die neuesten Produktpläne versendet
Verhinderung der Datenübertragung auf externe Seiten	Überwachung und/oder Unterbindung, dass sensiblen Informationen auf externen Webseiten oder Dateiserver übertragen werden
Kontrollierte Verwendung privater Webmail-Konten	Steuerung der Verwendung externer Webmail-Konten durch Mitarbeiter zur Verhinderung der Preisgabe sensibler Daten

McAfee und/oder andere in diesem Dokument enthaltene Marken sind eingetragene Marken oder Marken von McAfee, Inc. und/oder der Tochterunternehmen in den USA und/oder anderen Ländern. Die Farbe Rot in Verbindung mit Sicherheit ist ein Merkmal der McAfee-Produkte. Alle anderen eingetragenen und nicht eingetragenen Marken in diesem Dokument sind das alleinige Eigentum der jeweiligen Inhaber.  
© 2008 McAfee, Inc. Alle Rechte vorbehalten.  
5047al\_dtp\_dlp\_a\_use-case\_1208