McAfee DLP Prevent

Schützen Sie Ihre vertraulichen Daten mithilfe von Richtlinien

Je mehr Menschen elektronische Informationen gemeinsam nutzen, desto größer wird die Wahrscheinlichkeit, dass vertrauliche Daten unbeabsichtigt oder vorsätzlich an nicht autorisierte Personen weitergeleitet werden – und damit vertrauliche Unternehmensdaten einem Risiko aussetzen. Ob per E-Mail, Internet, Sofortnachrichten oder FTP: Es gibt zahlreiche Wege, auf denen Daten aus einem Unternehmen herausgeschleust werden können. Denn zum einen sind bestimmte Nachrichten sowie Datentransfers zulässig und sollten zum Schutz ihrer Vertraulichkeit verschlüsselt werden. Zum anderen gibt es aber auch Kommunikation, die zu keiner Zeit erfolgen darf und daher blockiert werden muss. Die wirksame Durchsetzung geeigneter Richtlinien zum richtigen Zeitpunkt trägt wesentlich zur Datensicherheit, zur Einhaltung gesetzlicher Bestimmung sowie zum Schutz geistigen Eigentums bei.

Hauptvorteile

Nutzung der bestehenden Infrastruktur

- Schutz der Unternehmens-E-Mails durch Integration von MTA-Gateways mittels SMTP mit X-Headern zur Blockierung, Abweisung, Verschlüsselung, Isolierung und Weiterleitung
- Schutz des Datenverkehrs durch Integration von ICAP-konformen Web-Proxys und Blockierung von Richtlinienverletzungen über HTTP, HTTPS, Sofortnachrichten, FTP sowie Webmail

Präventive Richtliniendurchsetzung bei allen Datentypen

- Schutz von über 300 Inhaltstypen
- Gewährleistung der Richtliniendurchsetzung bei offensichtlich sowie weniger offensichtlich vertraulichen Daten
- Erweiterung zur Unterstützung von mehreren Hunderttausend Verbindungen gleichzeitig

Klassifizierung, Analyse und Behebung von Datenverlustquellen

- Filterung und Kontrolle vertraulicher Daten zum Schutz vor bekannten und unbekannten Risiken
- Indexierung und Durchsetzung fein abgestimmter Sicherheitsrichtlinien für alle Inhaltstypen
- Umsetzung von Richtlinien für den internen Zugriff auf freigegebene Dateien zur Vermeidung des unberechtigten Zugangs zu Daten und Datenspeichern

Durchsetzung von Sicherheitsrichtlinien für bewegliche Daten

In allen Unternehmensbereichen greifen Mitarbeiter über mehrere Anwendungen und mithilfe einer Vielzahl von Protokollen auf freigegebene Daten zu. Zur Vermeidung unbeabsichtigt oder vorsätzlich herbeigeführter Datenverluste müssen Unternehmen ihre vertraulichen Daten mithilfe geeigneter Geschäftsabläufe präventiv davor schützen können, dass sie das eigene Netzwerk verlassen.

McAfee® Data Loss Prevention (DLP) Prevent ermöglicht die Richtliniendurchsetzung zum Schutz vor der nicht autorisierten Weitergabe von Daten per E-Mail, Webmail, Sofortnachrichten, Wikis, Blogs, Portalen, HTTP bzw. HTTPS und FTP. Dies geschieht durch die Integration von Message Transfer Agents (MTA)-Gateways mithilfe von SMTP (Simple Mail Transfer Protocol) oder ICAP-konformen Web-Proxys. Beim Auftreten einer Richtlinienverletzung können Sie mithilfe von McAfee DLP Prevent eine Reihe von Maßnahmen ergreifen, z. B. Verschlüsselung, Blockierung, Umleitung und Isolierung. Auf diese Weise können Sie die Einhaltung von Datenschutzvorschriften sicherstellen und das Risiko von Sicherheitsbedrohungen verringern.

Noch besserer Schutz durch die Integration von Web-Proxys und MTAs

McAfee DLP Prevent kann in Web-Proxys (über ICAP) und MTAs (über X-Header) integriert werden und dort die erforderlichen Aktionen auslösen. Da nicht autorisierte Transfers direkt auf Anwendungsebene blockiert werden, anstatt nur die TCP-Sitzung zu beenden (was keine Auswirkungen auf das Verhalten der Anwendung mit sich bringen würde), informiert McAfee DLP Prevent die den Transfer initiierende Anwendung darüber, dass die Übertragung aufgrund einer Richtlinienverletzung abgelehnt wurde. Da McAfee DLP Prevent „lernt“, welche Daten geschützt werden müssen und verhindert, dass die Anwendung das gleiche Verhalten erneut versucht, bedeutet dies noch besseren Datenschutz für Ihr Unternehmen.

Schutz von offensichtlich und weniger offensichtlich vertraulichen Daten

Dank der Möglichkeit, über 300 unterschiedliche Inhaltstypen zu klassifizieren, unterstützt McAfee DLP Prevent Sie dabei, die Sicherheit von Daten zu gewährleisten, die bekanntermaßen vertraulich sind (z. B. bei Steueridentifikations- und Kreditkartennummern sowie Finanzdaten). Zusätzlich lernt die

Spezifikationen

Systemdurchsatz
Bis zu 150 Mbit/s bei vollständiger Inhaltsanalyse, Indexierung und Speicherung

Netzwerkintegration
Integration in das Netzwerk als Off-Path-Appliance, die aktiv in den Datenpfad eingebunden ist und MTAs sowie ICAP-konforme Web-Proxys verwendet

Inhaltstypen
Unterstützung der Klassifizierung von über 300 Inhaltstypen:

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

Unterstützte Protokolle
Unterstützt HTTP, HTTPS, FTP sowie Sofortnachrichten-Protokolle über das ICAP-Protokoll eines ICAP-konformen Proxys. Informationen zu den von Ihrem Proxy unterstützten Protokollen erhalten Sie vom Anbieter Ihres Proxys. Unterstützt SMTP über die Integration von MTAs.

Integrierte Richtlinien

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

Lösung mit jedem Schritt, welche Daten oder Dokumente ebenfalls geschützt werden müssen (z. B. Dokumente mit hoch komplexem geistigem Eigentum). McAfee DLP Prevent enthält zahlreiche integrierte Richtlinien, die Vorschriften, zulässige Datennutzung sowie geistiges Eigentum umfassen. Über einen Abgleich mit vollständigen Dokumenten und Dokumentteilen können Sie eine umfangreiche Richtliniensammlung definieren, damit Sie alle vertraulichen Daten, bekannt oder unbekannt, schützen können.

Anpassung von Anzeigen und Berichten

Mithilfe der McAfee® ePolicy Orchestrator® (McAfee ePO™)-Verwaltungskonsole können Sie die Zusammenfassungen von Sicherheits-zwischenfällen und nachfolgenden Aktionen anhand von zwei beliebigen kontextbezogenen Zielpunkten anpassen. Dabei stehen Listen- und Detailansichten sowie Zusammenfassungen und Trendanalysen jederzeit auf Mausklick zur Verfügung. Zusätzlich enthält McAfee DLP Prevent zahlreiche voreingestellte Berichte, die angezeigt, für eine spätere Nutzung gespeichert oder für eine regelmäßige Aussendung geplant werden können.

Komplexe Datenklassifizierung

McAfee DLP Prevent ermöglicht Ihrem Unternehmen, verschiedenste vertrauliche Daten zu schützen – 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 Prevent eine äußerst genaue, detaillierte Klassifizierungs-Engine, die vertrauliche Informationen blockiert 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 Quell-Code-Dateien.
- **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.

Spezifikationen: McAfee DLP 5500-Appliance

Komponente	Anforderung
Prozessor	2 x Intel E5-2620 mit 6 Kernen, 15 MB Cache, 2,0 GHz, Intel QPI mit 7,20 GT/s
Arbeits-speicher	32 GB DDR3 mit 1.333 MHz
Netzteil	2 Hot-Swap-Netzteilmodule mit 760 W
Festplatten	8 Festplatten mit 2 TB, 7.200 U/min, SATA
Netzwerk-karte	1 Gb-Ethernet-E/A-Modul von Intel mit doppelter Kupferschnittstelle
IPMI	Intel Remote Management Module 4-Fernverwaltungsadapter (AXXRMM4)
Produktgröße	2 Rack-Einheiten (2 HE)

Spezifikationen: Virtuelle Maschinen

McAfee DLP Prevent kann als virtuelle Appliance in einer VMware-Umgebung ausgeführt werden. Im Folgenden finden Sie die Hardware-Mindestanforderungen für die virtuelle Appliance.

Komponente	Anforderung
Prozessor	4 virtuelle CPUs (Intel x86)
Arbeitsspeicher	16 GB RAM
Festplatte(n)	Festplatte 1: Mindestens 100 GB für VM-Software Festplatte 2: Mindestens 512 GB für virtuelles DLP-Abbild
Netzwerkports	4 virtuelle Netzwerkkarten
BIOS	VT-Thread-Aktivierung

McAfee. Part of Intel Security.
Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 37 07-0
www.intelsecurity.com