McAfee Data Loss Prevention Discover

Suche, Klassifizierung und Absicherung Ihrer vertraulichen Daten unabhängig vom Speicherort

Hauptvorteile

Erkennung potenzieller Datenverlustquellen

- Scannen Sie Informationen, die lokal oder in der Cloud gespeichert sind.
- Ermitteln Sie, wo vertrauliche Daten gespeichert sind und wem diese gehören.
- Durchsuchen und überprüfen Sie die erfassten Daten auf einer intuitiven Oberfläche.

Richtlinien und individuell angepasste Berichte

- Führen Sie Abfragen durch, und übertragen Sie die Ergebnisse in Schutzrichtlinien.
- Nutzen Sie voreingestellte Compliance-, Unternehmens- und Copyright-Richtlinien.
- Speichern Sie vertrauliche Daten parallel auf Datensicherheitssystemen.

Klassifizierung, Analyse und Beseitigung von Datenlecks

- Filtern und überwachen Sie sensible Daten mithilfe einer mehrstufigen Klassifizierung.
- Indexieren Sie sämtliche Inhalte, und überprüfen Sie diese vertraulichen Daten.
- Generieren und speichern Sie Signaturen, um Dokumente und die darin enthaltenen Daten auch bei Kopie oder Übertragung zu schützen.
- Senden Sie Warnmeldungen, wenn bestimmte Daten Schutzrichtlinien verletzen.

Die auf Laptops, freigegebenen Datei-Servern und in Cloud-Speichern gespeicherten sensiblen Daten stellen für Ihr Unternehmen unter Umständen ein Risiko dar. Riesige Datenmengen im Terabyte- oder gar Petabyte-Bereich müssen geschützt werden. Das ist insofern besonders schwierig, als vertrauliche Daten nicht immer als solche gekennzeichnet sind. Hinzu kommt, dass es in den meisten Unternehmen keine Möglichkeit gibt festzustellen oder zu überprüfen, ob vertrauliche Daten einem Risiko ausgesetzt sind. Genauso wenig lässt sich selbst bei Verwendung entsprechender Zugriffskontrollen erkennen, wohin diese Daten unter Umständen gelangt sein können. Zusätzliche Komplexität erfährt die Angelegenheit dadurch, dass vertrauliche Daten häufig unstrukturierte Daten wie zum Beispiel geistiges Eigentum umfassen, das schwieriger zu klassifizieren ist als strukturierte Daten wie Kreditkarten- oder Steueridentifikationsnummern. Mit McAfee® Data Loss Prevention (DLP) Discover können Sie Ihre sensiblen Daten finden sowie klassifizieren und feststellen, wie sie verwendet werden. Anschließend werden diese Daten vor Diebstahl oder Kompromittierung geschützt.

Was ist neu bei McAfee DLP Discover?

McAfee DLP Discover scannt und schützt jetzt auch Daten, die sich im Cloud-Speicher – der sogenannten Box – befinden. In der zentralen Verwaltungs-Software McAfee ePolicy Orchestrator® (McAfee ePO™) können auf einfache Weise Richtlinien definieren und Scans so planen, dass sie automatisiert und zu bestimmten Zeitpunkten ausgeführt werden. Außerdem haben Sie die Möglichkeit, Berichte zu Zwischenfällen zu generieren sowie detaillierte Analysen durchzuführen.

Funktionen und Highlights:

- Die reine Software-Variante von McAfee DLP Discover bietet zusätzliche Kosteneinsparungen, da weder Hardware noch eine VM-basierte Appliance erforderlich ist.
- Die Bereitstellung und Verwaltung erfolgt vollständig über die Software McAfee ePO. Dabei werden die gleichen Verwaltungserweiterungen und DLP-Richtlinien wie für DLP Endpoint verwendet.

intel Security

Spezifikationen

Inhaltstypen
Unterstützung der Klassifizierung von über 300 Inhaltstypen, wie:

- Box (Cloud-Datenspeicher)
- Microsoft Office-Dokumente
- Multimediadateien
- Quell-Code
- Design-Dateien
- Archive
- Verschlüsselte Dateien
- Integrierte Richtlinien
- Geistiges Eigentum

Unterstützte Datenspeicher

- Common Internet File System (CIFS) / Server Message Block (SMB)[1]
- Network File System (NFS)
- HTTP / HTTPS
- FTP / FTPS
- Microsoft SharePoint[1]
- EMC Documentum
- Datenbanken: Microsoft SQL, Oracle, DB2, MySQL Enterprise

Dokumentenregistrierung
Es können Dokumente auf beliebigen Datenspeichern registriert werden. Die Signaturen der registrierten Dokumente können lokal zur Erkennung der nicht autorisierten Weitergabe vertraulicher Daten verwendet oder anderen McAfee DLP-Appliances zur Verfügung gestellt werden.

- Die Lösung ist vollständig auf die Klassifizierungsfunktionen von DLP Endpoint abgestimmt.
- Mit Windows Server 2008 und Windows Server 2012 kompatibel.
- Unterstützt verteilte Bereitstellungen, die Leerlauf-Kapazitäten auf vorhandenen Servern nutzen und über einen großen geografischen Bereich verteilt sein können.
- Mit der Lizenz für die DLP Discover-Appliance 9.3.x sowie mit der reinen Software-Version von DLP Discover 9.4 kompatibel.

Verlust vertraulicher Daten vermeiden

Von Quell-Code über Geschäftsgeheimnisse bis hin zu strategischen Geschäftsplänen – geistiges Eigentum und andere Informationswerte spielen eine wichtige Rolle für Ihre Marke, Ihren Ruf und Ihren Wettbewerbsvorteil. Dem Schutz Ihrer Daten während einer Übertragung kommt damit eine besondere Bedeutung zu. Aber Ihr größtes Augenmerk sollte auf den Schutz vertraulicher Daten vor nicht autorisiertem Zugriff oder unerlaubten Kopien gerichtet sein. So besteht Ihre erste Aufgabe darin, festzustellen, wo derartige Daten gespeichert werden.

McAfee DLP Discover unterstützt Ihr Unternehmen beim Schutz vor Datenverlusten. Im Gegensatz zu herkömmlichen Lösungen, bei denen Sie genau wissen müssen, was Sie eigentlich schützen möchten, bietet Ihnen McAfee DLP Discover einen umfassenden Schutz der offensichtlich vertraulichen Daten sowie eine Möglichkeit zum Auffinden der weniger offensichtlichen Informationen.

Schützenswerte Daten bestimmen

Zur Feststellung von Datenverlustquellen und Weitergaberisiken kann McAfee DLP Discover so konfiguriert werden, dass bestimmte Datenspeicher untersucht und Datenbereiche definiert werden, die einem besonderen Schutz unterliegen sollen. Darüber hinaus werden sämtliche von McAfee DLP Discover durchsuchten Daten indexiert und für den Zugriff über eine intuitive Oberfläche freigegeben. Dies ermöglicht die kurzfristige Suche nach möglicherweise vertraulichen Daten und erleichtert das Verständnis, wem diese Daten gehören und wo sie gespeichert sind.

Schutzrichtlinien festlegen

Sobald Sie wissen, um welche Daten es sich handelt, können Sie diese mithilfe von McAfee DLP Discover entsprechend schützen. McAfee DLP Discover beinhaltet intuitive und zentrale Funktionen zur Erstellung und Verwaltung von Richtlinien sowie zur Berichterstattung, die Ihnen mehr Kontrolle über Ihre Informationsschutzstrategie für gespeicherte Daten geben. Zu den wichtigsten Vorteilen der Richtlinien, Regeln und Klassifizierungen mit McAfee DLP Discover zählen:

- Zahlreiche integrierte Richtlinien für den sofortigen Einsatz des Produkts ohne großen Konfigurationsaufwand
- Mächtiges Regelerstellungsmodul, das mit einfach strukturierten Daten (z. B. Kreditkarten- oder Steueridentifikationsnummern) ebenso umgehen kann wie mit komplexen Informationen (geistigem Eigentum)
- Einfache Regelerstellung und -validierung durch Umsetzung der Analysen von Suchergebnissen in Schutzregeln

Berichterstattung
Das leistungsfähige Analysemodul zur Anzeige von Datenschutz- und Suchergebnissen ermöglicht die Anpassung von Zusammenfassungen anhand von zwei kontextbezogenen Zielpunkten. Dabei stehen Listen- und Detailansichten sowie Zusammenfassungen und Trendanalysen zur Verfügung. Das System verfügt über mehr als 20 integrierte und anpassbare Berichte.

- Integration in parallel implementierte Datenschutzfunktionen zur Gewährleistung von konsistentem Schutz
- Ausschluss von allgemein zugänglichen Dokumenten und allgemeinen Texten zur Vermeidung von Fehlermeldungen bei unkritischen Daten

Netzwerk auf Datenschutzverletzungen prüfen

Nach Definition der Richtlinien kann McAfee DLP Discover angewiesen werden, die Netzwerkressourcen regelmäßig auf Datenschutzverletzungen zu untersuchen. Zur Einrichtung dauerhafter, täglicher, wöchentlicher oder monatlicher Scan-Vorgänge stehen flexible Planungsfunktionen zur Verfügung.

McAfee DLP Discover durchsucht automatisch sämtliche verfügbaren Ressourcen auf Richtlinienverletzungen, einschließlich Laptops, Desktops, Server, Dokumentspeicher, Portale und Dateitransferpunkte. Die zu durchsuchenden Datei-Ressourcen können anhand ihrer IP-Adressen, Subnetze, Adressbereiche oder Netzwerkpfade zu Scan-Gruppen zusammengefasst werden. Außerdem haben Sie die Möglichkeit, die Scan-Vorgänge anhand bestimmter Parameter auf spezifische Bereiche zu konzentrieren, wie z. B. die „Eigenen Dateien“ aller Benutzer und die Systemverzeichnisse nicht. Oder Sie können nach Dateien suchen, die bestimmten Benutzern gehören oder einen bestimmten Typ bzw. eine besondere Größe aufweisen.

Verletzungen überprüfen und beseitigen

McAfee DLP Discover verhindert oder minimiert die Verbreitung sensibler Daten durch einen integrierten Ereignis-Workflow sowie Fall-Management. Wenn McAfee DLP Discover feststellt, dass eine Schutzrichtlinie verletzt wurde, werden Ereignisprotokolle erstellt und Benachrichtigungen versendet.

Von McAfee DLP Discover erstellte Zwischenfallprotokolle lassen sich dem Fall-Management hinzufügen, damit Experten aus verschiedenen Unternehmensbereichen geeignete Maßnahmen ergreifen können. Zudem ermöglichen Risiko-Dashboards den Sicherheitsbeauftragten die Anzeige der Profile von Richtlinienverletzungen sowie die Erstellung von Berichten zu bestimmten Parametern von ruhenden Daten.

Gespeicherte Daten erfassen und analysieren

Zusätzlich zur Untersuchung von Netzwerkressourcen auf Richtlinienverletzungen indexiert McAfee DLP Discover sämtliche Inhalte der im Netzwerk gespeicherten ruhenden Daten und ermöglicht den Sicherheitsbeauftragten die Abfrage und Auswertung der Informationen, die zum Verständnis der vertraulichen Daten von Bedeutung sind. Mithilfe von McAfee DLP Discover können Sie ihre vertraulichen Daten schnell und einfach erfassen sowie feststellen, wie diese verwendet werden, wem sie gehören, wo sie gespeichert werden und wohin sie ggf. transferiert wurden.

Komplexe Daten klassifizieren

McAfee DLP Discover 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 der Eingaben aus diesen Objektklassifizierungsverfahren kann McAfee DLP Discover eine äußerst genaue, mehrstufige Klassifizierung vornehmen, anhand der die vertraulichen Daten gefiltert und der Zugriff darauf gesteuert werden kann. Mithilfe der Klassifizierung sind zudem Suchvorgänge möglich, mit denen versteckte oder unbekannte Risiken erkannt werden können. Zu den Objektklassifizierungsverfahren zählen:

- Mehrstufige Klassifizierung: Fasst sowohl Kontextdaten als auch Inhalte in einem hierarchischen Format zusammen.

Spezifikationen: Reine Software-Lösung

McAfee DLP Discover ist als Software-Version verfügbar. Die folgenden Angaben sind die Mindestanforderungen an die Systeme.

Hardware-Anforderungen

- Prozessor: Intel Core 2 (64-Bit)
- Arbeitsspeicher: mindestens 4 GB
- Festplattenspeicher: mindestens 100 GB

Unterstützte Plattformen

- Windows Server 2008 R2 Standard (64-Bit-Version)
- Windows Server 2012 Standard (64-Bit-Version)
- Windows Server 2012 R2 Standard (64-Bit-Version)

Unterstützte Virtualisierungssysteme

- vSphere ESXi 5.0 Update 2
- vCenter Server 5.0 Update 2

McAfee ePO-Software und -Agenten

- McAfee ePO 4.6.8 oder höher und 5.1 oder höher
- McAfee Agent 4.8.2 oder höher und 5.0 oder höher

- 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.

Spezifikationen: McAfee DLP 5500-Appliance

McAfee DLP Discover ist als physische bzw. virtuelle Appliance verfügbar. Im Folgenden finden Sie die Spezifikationen zur Appliance.

Komponente	Beschreibung
Prozessor	2 x Intel E5-2620 mit 6 Kernen, 15 MB Cache, 2,0 GHz, Intel QPI mit 7,20 GT/s
Arbeitsspeicher	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
Netzwerkkarte	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 Discover 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
Netzwerk	4 virtuelle Netzwerkkarten
BIOS	VT-Thread-Aktivierung

1. Die reine Software-Version von McAfee DLP Discover 9.4 unterstützt derzeit CIFS, Microsoft SharePoint 2010 und Microsoft SharePoint 2013.

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