

McAfee Network DLP Discover

(zuvor „Reconnex iGuard Discover“)

Erkennen und schützen Sie vertrauliche Daten

Die auf Laptops, freigegebenen Dateiservern und Portalen oder in Dokumentenmanagementsystemen gespeicherten Daten stellen für Unternehmen und Organisationen unter Umständen ein Risiko dar. Riesige Datenmengen – in unserer heutigen Zeit im Terabyte oder gar Petabytebereich – müssen geschützt werden. Dies 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 normalerweise Ressourcen geistigen Eigentums sind, die schwieriger zu klassifizieren sind als eindeutige Daten wie Kreditkarten- oder Sozialversicherungsnummern.



Hauptvorteile

Erkennung von Datenlecksrisiken

- Scannen Sie Daten auf allen verfügbaren Datenträgern.
- Stellen Sie fest, wo vertrauliche Daten gespeichert sind und wem diese gehören.
- Durchsuchen und überprüfen Sie Scandaten auf einer intuitiven Oberfläche.

Erstellen Sie 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.

Klassifizieren, analysieren und beseitigen Sie Datenlecks

- Filtern und überwachen Sie vertrauliche Daten mithilfe einer mehrstufigen Klassifizierung.
- Indexieren Sie sämtliche Inhalte. 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.

Verlust vertraulicher Daten vermeiden

Von Quellcode über Geschäftsgeheimnisse bis hin zu strategischen Unternehmensplänen sind geistiges Eigentum und andere Daten für Ihre Marke, Ihr Ansehen in der Öffentlichkeit und Ihre Wettbewerbsvorteile von entscheidender Bedeutung. Dem Schutz Ihrer Daten während einer Übertragung kommt damit eine besondere Bedeutung zu. Aber Ihr vorderstes Augenmerk sollte auf den Schutz vertraulicher Daten vor nicht autorisiertem Zugriff oder Verlagerung gerichtet sein. So besteht Ihre erste Aufgabe darin, festzustellen, wo derartige Daten gespeichert werden.

McAfee Network DLP (Data Loss Prevention)

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

Schützenswerte Daten bestimmen

Zur Feststellung von Datenlecks und Weitergabrisiken kann McAfee Network 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 Network DLP Discover durchsuchten Daten indexiert und für einen Zugriff mithilfe einer intuitiven 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 mithilfe von McAfee Network DLP Discover diese Daten entsprechend schützen. Hierzu bietet McAfee Network DLP Discover intuitive und einzigartige Funktionen zur Richtlinien- und Berichterstellung sowie zur Verwaltung, damit Sie eine größere Kontrolle über die Schutzstrategien für Ihre gespeicherten Daten ausüben können. Zu den wichtigsten Vorteilen der Richtlinien, Regeln und Klassifizierungen mit McAfee Network DLP Discover zählen:

- Zahlreiche integrierte Richtlinien für den sofortigen Einsatz des Produkts ohne großen Konfigurationsaufwand
- Mächtige Regelerstellungs-Engine, die mit einfach strukturierten Daten (Kreditkarten- bzw. Sozialversicherungsnummern) ebenso umgehen können wie mit komplexen Informationen (geistigem Eigentum).
- Einfache Regelerstellung und -validierung durch Umsetzung der Analysen von Suchergebnissen in Schutzregeln.
- Integration in parallel implementierte Datenschutzfunktionen zur Sicherstellung einer konsistenten Sicherheitsleistung.
- Ausschluss von allgemein zugänglichen Dokumenten und allgemeinen Texten zur Vermeidung von Fehlermeldungen bei unkritischen Daten.

Spezifikationen

Erfassung und Indexierung

- Indexierung von bis zu 5 TB an Daten und bis zu 2 Millionen Dokumente auf einer McAfee Network DLP 1650-Appliance (1U).
- Indexierung von bis zu 50 TB an Daten und bis zu 25 Millionen Dokumente auf einer McAfee Network DLP 3650-Appliance (3U).

Systemdurchsatz

- Inhaltserkennung mit bis zu 500 Mbit/Sek.
- Indexierung mit bis zu 150 Mbit/Sek.

Inhaltstypen

Unterstützung der Klassifizierung von über 300 Inhaltstypen, wie:

- Office-Dokumente
- Multimediadateien
- Quellcode
- Design-Dateien
- Archive
- Verschlüsselte Dateien
- Integrierte Richtlinien
- Geistiges Eigentum

Unterstützte Datenspeicher

- Common Internet File System (CIFS) / Server Message Block (SMB)
- Network File System (NFS)
- HTTP / HTTPS
- FTP
- Microsoft Sharepoint
- EMC Documentum

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 Network DLP-Appliances zur Verfügung gestellt werden.

Berichte

Leistungsfähige Analyse-Engine 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.

Überprüfung des Netzwerks auf Datenschutzverletzungen

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

McAfee Network DLP Discover durchsucht automatisch sämtliche verfügbaren Ressourcen auf Richtlinienverletzungen, einschließlich Laptops, Desktops, Server, Dokumentspeicher, Portale und Dateitransferpunkte. Die zu durchsuchenden Dateiressourcen können anhand ihrer IP-Adressen, Subnets, 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 Network DLP Discover verhindert bzw. minimiert die nicht autorisierte Weitergabe vertraulicher Daten mithilfe integrierter Zwischenfall-Workflows und Fall-Management-Vorgängen. Wenn McAfee Network DLP Discover feststellt, dass eine Schutzrichtlinie verletzt wurde, so werden Zwischenfallprotokolle erstellt und Benachrichtigungen versendet. Von McAfee Network DLP Discover erstellte Zwischenfallprotokolle können dem Fall-Management hinzugefügt werden. Dadurch können Experten aus mehreren Bereichen eines Unternehmens entsprechende Maßnahmen ergreifen. 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

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

Komplexe Datenklassifizierung

McAfee Network DLP Discover ermöglicht Ihrem Unternehmen, vertrauliche Daten unterschiedlicher Typen zu schützen: Von allgemeinen Daten eines bestimmten Formats bis hin zu komplexem und hoch variabelm geistigen Eigentum. Durch die Kombination der Eingaben aus diesen Objektklassifizierungsverfahren kann McAfee Network DLP Discover eine äußerst genaue, mehrstufige Klassifizierung vornehmen, anhand der die vertraulichen Daten gefiltert und ihr Zugang gesteuert werden kann. Außerdem ermöglicht die Klassifizierung die Durchführung von Suchvorgängen, 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.
- 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.

