DATENBLATT

McAfee-Schutz vor Datenlecks zwischen Endgeräten und Cloud

Einheitlicher Datenschutz

Unternehmen aller Größen nutzen Cloud-basierte Dienste wie Microsoft Office 365, um ihren Mitarbeitern mehr Flexibilität und einfacheren Zugriff auf wichtige Geschäftsanwendungen zu geben. Lokale Datenschutzlösungen bieten meist keinen Überblick über Daten in Cloud-Diensten wie Office 365 und können die Zusammenarbeit oder Freigabe in der Cloud nicht kontrollieren. Viele Unternehmen haben vor, eine separate Datenschutzlösung für ihre Cloud-Umgebung zu implementieren. Dadurch würden sie jedoch ihre Richtlinien, Berichte und die Reaktion auf Zwischenfälle fragmentieren, was zu höherem Arbeitsaufwand und uneinheitlichem Datenschutz zwischen Geräten, Netzwerken und Cloud-Diensten führen würde.

McAfee®-Schutz vor Datenlecks zwischen Endgeräten und Cloud bietet durch die Integration zweier branchenweit führender Technologien – McAfee® Data Loss Prevention (McAfee DLP) und McAfee® MVISION Cloud – einheitlichen Datenschutz für Endgeräte, Netzwerke und die Cloud. Dank dieser Integration erhalten Unternehmen nahtlosen und einheitlichen Datenschutz, der das Risiko von Datenverlusten minimiert und maximale betriebliche Effizienz gewährleistet.

Die Ineffizienz fragmentierter Datenschutzlösungen

Die Implementierung von DLP (Data Loss Prevention, Schutz vor Datenverlust) in der Cloud erforderte bislang einen Neuaufbau der für lokale Kontexte erstellten DLP-Regeln für die Cloud. Den lokalen DLP-Regeln fehlte zudem der Kontext Cloud-eigener Zusammenarbeit oder die Freigabe für Dritte in Cloud-Diensten. Dies führte zu enormem Zeitaufwand für die Replikation schon vorhandener Arbeiten, die bereits für Daten auf Geräten und im Netzwerk durchgeführt waren, wobei die Richtlinienerzwingung aufgrund unterschiedlicher DLP-Module möglicherweise nicht einheitlich erfolgte. Lokale DLP-Lösungen konnten Datenverluste durch Zusammenarbeit oder freigegebene Links in der Cloud nicht erkennen.

Wichtige Vorteile

Nahtlose Integration

- Einmalige Klassifizierung der Daten in McAfee ePO und Nutzung dieser Klassifizierung für Geräte, Netzwerke und Cloud-Kontexte
- Vernetzung von lokalem und Cloud-DLP kann mit einem Klick und in weniger als einer Minute erfolgen

Einheitlicher Schutz vor Datenverlust

- Ein gemeinsames Richtlinien- und Klassifizierungsmodul wird für mehrere Umgebungen eingesetzt
- Keine Notwendigkeit von Änderungen in mehr als einer Konsole

Zentrale Übersicht für gesamte Verwaltung von Zwischenfällen und Berichterstellung

- Zentrale Verwaltung von Zwischenfällen in verschiedenen Umgebungen
- Keine Notwendigkeit zum Wechsel zwischen Konsolen zum Anzeigen von Vorfällen und Berichten

Folgen Sie uns

Einfaches Vernetzen und Synchronisieren des Schutzes vor Datenverlust lokal und in der Cloud

McAfee® ePolicy Orchestrator® (McAfee ePO™) vereinfacht den Schutz vor Datenverlust vom Endgerät bis zur Cloud. Durch die Zusammenarbeit von MVISION Cloud und McAfee ePO können Sie Daten in jedem Cloud-Dienst schneller als je zuvor schützen und erhalten den vollständigen Kontext von Zusammenarbeit und Freigabe innerhalb der Cloud. Die Vernetzung der beiden Lösungen kann mit einem Klick und innerhalb von weniger als einer Minute erfolgen.[1] Die in McAfee ePO erstellten DLP-Regeln für Ihre Geräte und Netzwerke werden an MVISION Cloud übertragen. Von hier aus können sie für jeden Cloud-Dienst und jeden Datenverkehr innerhalb der Cloud angewendet werden, der Ihr Netzwerk passiert. Ihre Datenklassifizierungen werden synchronisiert und gewährleisten einheitlichen Schutz vor Datenkompromittierung auf Endgeräten und in der Cloud. Alle Zwischenfälle werden an McAfee ePO gesendet, sodass Sie einen einheitlichen DLP-Workflow vom Gerät bis zur Cloud nutzen können.

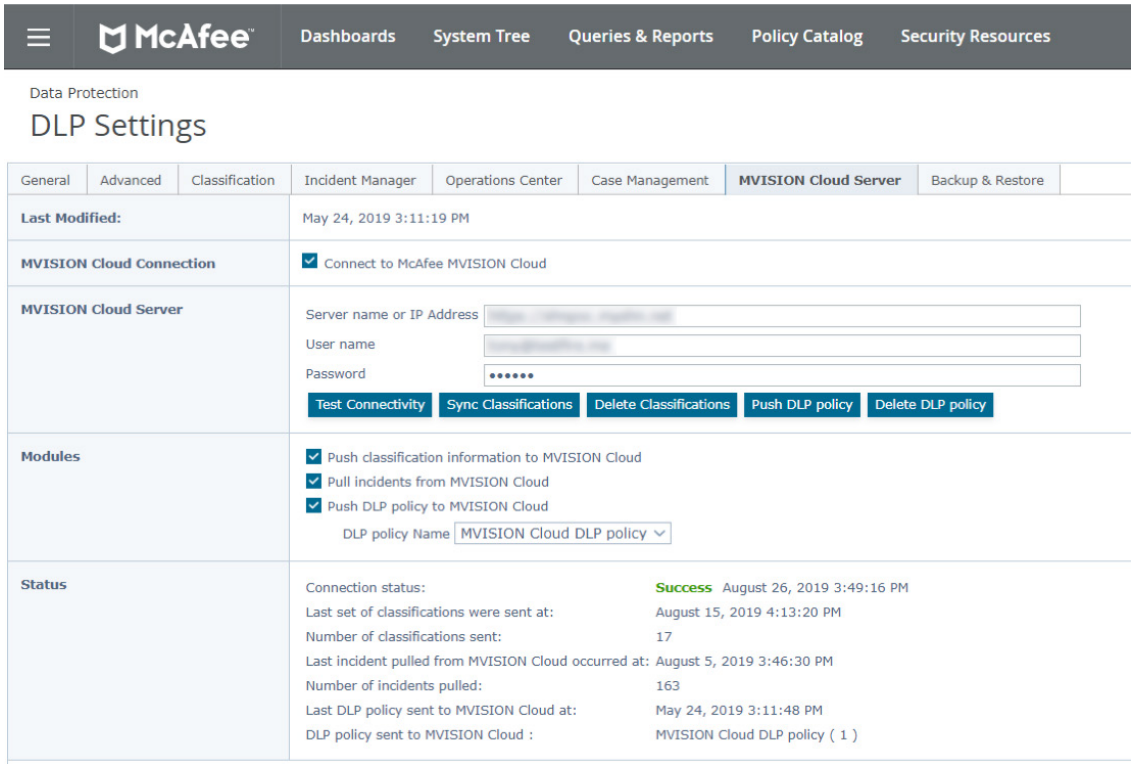

Abbildung 1. DLP-Richtliniensynchronisierung für MVISION Cloud in McAfee ePO

Betriebliche Effizienz durch Schutz vor Datenverlust vom Endgerät bis zur Cloud für Unternehmen

Kunden mit McAfee ePO profitieren von dieser Integration, da sie die Durchsetzung von DLP in Cloud-Diensten sowie die Optimierung ihrer Abläufe weitgehend vereinfachen können. Beispielsweise musste ein großer Lebensmitteldienstleister, der McAfee DLP auf seinen Endgeräten und Netzwerkfreigaben nutzte, den Speicherort der eigenen Daten in der Cloud lokalisieren und eine Schutzstrategie entwickeln. Das Unternehmen setzte bei McAfee® Web Gateway an und analysierte seinen Web-Datenverkehr, um die am häufigsten von seinen Benutzern angesteuerten Ziele sowie die Speicherorte der Unternehmensdaten in der Cloud zu bestimmen. Dadurch stellte das Unternehmen fest, dass der überwiegende Teil seiner Daten in Microsoft Office 365 konzentriert war.

Die Anforderungen dieses Unternehmens an den Datenschutz in der Cloud blieben die gleichen wie bei lokaler Nutzung, doch der unterschiedliche Kontext wie Dateifreigabe und Zusammenarbeit in der Cloud ergab neue Herausforderungen. Beispielsweise musste das Unternehmen On-Demand-Scans seiner Daten in Office 365 ebenso wie lokal durchführen und gleichzeitig DLP-Regeln für in und aus Office 365 übertragene Daten durchsetzen, die es nur in der Cloud gab und die nicht von der Netzwerkübersicht erfasst wurden. Es wurde festgelegt, dass ein CASB (Cloud Access Security Broker) die beste Lösung zur Erfüllung dieser Anforderungen war, und mehrere Angebote auf dem Markt untersucht. Letztendlich entschied sich das Unternehmen aufgrund der engen Integration der bestehenden DLP-Regeln in McAfee ePO für MVISION Cloud. Aus McAfee ePO heraus übertrug das Sicherheitsteam lokale Datenklassifizierungen an MVISION Cloud und erstellte dann mithilfe dieser vordefinierten Klassifizierungen Richtlinien für Office 365. Jetzt besitzt das Unternehmen eine zentrale Stelle zur Verwaltung der Datenklassifizierungen, DLP-Zwischenfälle auf Geräten und in der Cloud sowie Berichte über den Web-Datenverkehr von McAfee Web Gateway. Das alles war über McAfee ePO möglich.

„Wir entschieden uns für McAfee MVISION Cloud als unseren CASB, da wir eine Übersicht erhalten, wohin unsere Daten übertragen werden und wer darauf Zugriff hat. Zudem können wir ohne Probleme die damit die Risiken der einzelnen Cloud-Dienste verstehen.“

– CISO bei einem weltweiten IoT-Hersteller

Zentrale Verwaltung von Zwischenfällen und Berichterstellung

Mit McAfee ePO erhalten Sie einen zentralen und einheitlichen Überblick für die Verwaltung aller DLP-Verstöße und die Berichterstellung. Unabhängig davon, ob die DLP-Verstöße von Geräten im Unternehmen oder Cloud-Anwendungen verursacht wurden, muss für die Anzeige von Zwischenfällen sowie die Generierung von Berichten nicht mehr zwischen Konsolen gewechselt werden. Dank der Übersicht aller vertraulichen Daten in verschiedenen Umgebungen verringert die zentrale Konsole die Komplexität von Auditing- und Vorschriften-Compliance-Prozessen.

Zusammenfassung

Da die Menge an Daten täglich wächst, die in die und aus der Cloud übertragen werden, sind einheitliche DLP-Richtlinien für den Schutz von Daten vor Kompromittierung wichtiger als jemals zuvor. Dabei spielt es keine Rolle, ob unternehmenseigene Endgeräte, unverwaltete Geräte, das Netzwerk oder Cloud-Anwendungen als Kompromittierungsvektor dienen.

McAfee-Schutz vor Datenlecks zwischen Endgeräten und Cloud bietet Unternehmen nahtlosen und einheitlichen Datenschutz für mehrere Umgebungen. Durch die größere betriebliche Effizienz sparen sie Zeit und können zudem das Risiko von Datenverlusten minimieren.

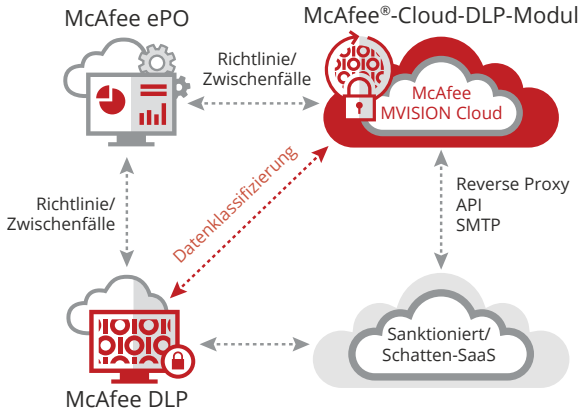

Abbildung 2. Allgemeine Architektur für die Ereignisverwaltung für McAfee-Schutz vor Datenlecks zwischen Endgeräten und Cloud

Weitere Informationen

Weitere Informationen erhalten Sie unter **www.mcafee.com/enterprise/de-de/products/data-protection-products.html**.

1. Basierend auf einheitlichen internen McAfee-Labortests.

McAfee
Together is power.

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