McAfee Cloud Visibility – Community Edition

Überblick über die Nutzung von Cloud-Anwendungen, damit verbundene Risiken, übertragene vertrauliche Daten und den Endgerätestatus (für Kunden mit McAfee DLP oder einer unserer Webschutz- oder Verschlüsselungslösungen)

Hauptvorteile

- Für Kunden mit McAfee DLP oder einer unserer Webschutz- oder Verschlüsselungslösungen
- Kostenloser Dienst
- Überblick über die Schatten-IT
- Erkennung von mehr als 5.000 Cloud-Diensten
- Analyse der Risiken
- Gemeinsame Risikodatenbank für Web- und Datenschutz
- Überwachung der Übertragung vertraulicher Daten
- Kontrolle des Endgerätestatus
- Einfache Aktivierung und Verwendung
- Nutzung der Software McAfee ePO
- Integriert sich in Endgeräte-, Web- und Datenschutzlösungen

Unternehmensmitarbeiter und interne Entwickler nutzen immer häufiger Cloud-Dienste – Microsoft Office 365 (O365), Box oder Amazon Web Services (AWS) – zur Steigerung der Produktivität und Vereinfachung der Zusammenarbeit. Daher ist die nicht autorisierte Nutzung dieser Cloud-basierten Dienste zu einem derart verbreiteten Phänomen geworden, dass es einen eigenen Namen bekommen hat: Schatten-IT. Doch selbst wenn bestimmte Cloud-Dienste zugelassen werden, haben IT- und Sicherheitsadministratoren kaum oder keinen Überblick über die Nutzung dieser Dienste, ihre Benutzer und – wichtiger noch – die dabei hochgeladenen sowie gespeicherten Daten. Wenn nicht autorisierte Personen Zugriff auf Daten in Cloud-Diensten erhalten, kann das bei den betroffenen Unternehmen zu Datenkompromittierungen, Compliance-Verstößen und Rufschädigungen führen. Zur Minimierung der Risiken benötigen Unternehmen eine Möglichkeit, sowohl den Cloud-Zugang als auch die vertraulichen Daten zu überwachen, die in die und aus der Cloud übertragen sowie von Cloud-Anwendungen verarbeitet werden. McAfee® Cloud Visibility – Community Edition löst diese Herausforderung.

McAfee Cloud Visibility – Community Edition stellt über ein zentrales Dashboard einen Überblick über die im Unternehmen genutzten Cloud-Anwendungen bereit und steht Kunden mit McAfee DLP oder einer unserer Webschutz- oder Verschlüsselungslösungen kostenlos zur Verfügung. Dieser Dienst bietet folgende Möglichkeiten:

- Erkennung autorisierter und nicht autorisierter Cloud-Anwendungen, die von Mitarbeitern genutzt werden
- Aufdeckung von Risiken im Zusammenhang mit Cloud-Anwendungen basierend auf Risikoindikatoren
- Überwachung vertraulicher Daten, die zwischen Benutzern und Cloud-Anwendungen übertragen werden
- Kontrolle des Status von Endgeräten im Kontext von Bedrohungen, Datenlecks sowie Datendiebstahl

Was macht McAfee Cloud Visibility – Community Edition einzigartig?

McAfee Cloud Visibility – Community Edition nutzt eine zentrale Risikodatenbank für Web- sowie Datenschutz und bietet einen Überblick über die Nutzung von Cloud-Anwendungen, zugehörige Risiken, übertragene vertrauliche Daten sowie den Endgerätestatus. Hier erhalten Sie einen wirklich zentralen Überblick mit einer Endgerät-zu-Cloud-Übersicht.

intel Security

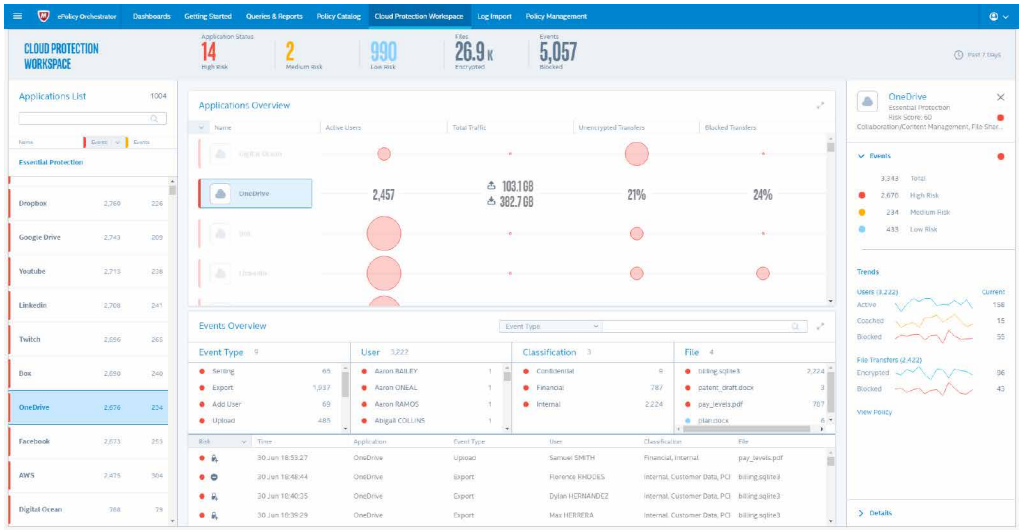

Abbildung 1. McAfee Cloud Protection Workspace

Erkennung autorisierter und nicht autorisierter Cloud-Anwendungen, die von Mitarbeitern genutzt werden

McAfee Cloud Visibility – Community Edition kann über die Software McAfee ePolicy Orchestrator® (McAfee ePO™) Cloud genutzt werden, die sich nahtlos in andere McAfee-Lösungen integriert. Eine wichtige Funktion ist McAfee Cloud Protection Workspace, das eine schnelle Übersicht der Cloud-Anwendungsnutzung gibt. Die neue Benutzerführung erleichtert es Administratoren, verschiedene Details von im Unternehmen eingesetzten Cloud-Anwendungen anzuzeigen, und stellt die Anzahl der aktiven Benutzer, den gesamten Datenverkehr sowie verschlüsselte und blockierte Datenübertragungen für eine Liste von Cloud-Anwendungen übersichtlich dar. Zudem ermöglicht McAfee Cloud Protection Workspace die weitere Untersuchung bestimmter Ereignistypen (z. B. Export, Upload und Freigabe), Benutzer, Klassifizierungen oder Dateien.

Aufdeckung von Risiken im Zusammenhang mit Cloud-Anwendungen basierend auf Risikoindikatoren

McAfee Cloud Visibility – Community Edition ermittelt die Risiken anhand folgender Parameter:

- Unternehmensprofil der Cloud-Anwendung
- Rechtliche Aspekte wie Endbenutzer-Lizenzvertrag (EULA), Service-Bedingungen und Datenschutzrichtlinien
- Compliance (hält die Cloud-Anwendung nationale oder internationale Datenanforderungen ein)
- Intel® Security-Auswertungen
- Authentifizierungs- und Zugriffskontrollen
- Zuverlässigkeit und Sicherheit des Dienstes
- Benutzeraktivitäten

Diese Übersichtlichkeit ermöglicht Risikoanalysen zur Abwehr von Bedrohungen, indem Cloud-Anwendungen identifiziert und entsprechend ihrer Risikowerte in absteigender Reihenfolge sortiert werden. Dadurch können Administratoren Maßnahmen priorisieren und Risiken verstehen, die ihnen zuvor unbekannt waren.

Überwachung vertraulicher Datenflüsse zwischen Benutzern und Cloud-Anwendungen

Ihr Administrator erhält eine umfassende Übersicht vom Endgerätestatus bis zu den Cloud-Benutzeraktivitäten. Details dazu, wie und wohin vertrauliche Daten übertragen werden, erleichtern die Planung der notwendigen Kompromittierungschutzrichtlinien für Endgeräte, sodass vertrauliche Daten besser kontrolliert werden können. Ebenfalls sehr nützlich ist die Möglichkeit, den Fluss bestimmter vertraulicher Daten (z. B. PCI und personenbezogene Daten) zwischen Cloud-Anwendungen und Benutzern zu überwachen sowie die Risikowerte im Zusammenhang mit vertraulichen Daten in Cloud-Anwendungen zu korrelieren.

Kontrolle des Status von Endgeräten im Kontext von Bedrohungen, Datenlecks sowie Datendiebstahl

Die Möglichkeit zur kontinuierlichen Überwachung des Endgerätestatus in Bezug auf Malware-Schutz, Schutz vor Datenkompromittierung sowie Verschlüsselungstechnologien ermöglicht die Implementierung eines umfassenden Bedrohungsschutzplans. Sie können bereits geschützte Endgeräte ermitteln und feststellen, welche noch Malware-Schutz benötigen. Zudem ist es möglich, Endgeräte ohne Verschlüsselungslösungen (unverzichtbar bei Endgerätediebstahl) und ohne Schutz vor Datenkompromittierung zu finden.

Komponente	Vorteile
Erkennung von Cloud-Anwendungen Wichtig für Kunden mit McAfee Web Gateway und McAfee DLP	• Detaillierter Einblick in die Nutzung von Cloud-Diensten wie O365, AWS und Box • Erkennung der Datenmengen, die in und aus zulässigen sowie nicht autorisierten Anwendungen übertragen werden • Überblick über die Benutzer und die von ihnen verwendeten Cloud-Anwendungen
Risikobewertung Wichtig für Kunden mit McAfee Web Gateway und McAfee DLP	• Nutzung von Risikokategorien und anwendungsbasierter umfassender Logik, die eine Vielzahl von Faktoren berücksichtigt • Vereinfachte Überwachung durch Unterteilung in Kategorien mit hohem, mittlerem und geringem Risiko • Aufzeigen von Möglichkeiten zur Kontrolle risikoreicher Benutzer und Geräte
Verteilung vertraulicher Daten und Ereignisüberwachung Wichtig für Kunden mit McAfee DLP	• Verhinderung von Datenkompromittierung durch genaue Überwachung der Endgeräteaktivitäten • Erkennung, ob bestimmte Aktivitäten blockiert oder zugelassen werden sollen
Zentrale Kontrolle und Überwachung mit McAfee ePolicy Orchestrator Cloud	• Verwaltung über eine zentrale Oberfläche mit McAfee ePO Cloud für Cloud-basierte SaaS-Anwendungen sowie PaaS- und IaaS-Cloud-Dienste • Integriert sich in lokale Sicherheitstechnologien • Zentrale Verwaltung mehrerer Benutzerkonten für verschiedene Cloud-Plattformen • Einfache Bereitstellung sowie Durchsetzung von Cloud-Dienstrichtlinien zur Einhaltung gesetzlicher und rechtlicher Bestimmungen
Zustandsprüfung der Endgeräte Wichtig für Kunden mit Endgeräten	• Erkennung, welche Endgeräte vor Bedrohungen geschützt sind und welche Malware-Schutz benötigen • Erfassung, welche Endgeräte Verschlüsselung benötigen, die zum Schutz der Daten bei Diebstahl unverzichtbar ist • Überprüfung, welche Endgeräte über Technologien zum Schutz vor Datenkompromittierung verfügen

Aktivierung dieses kostenlosen Services hier: www.mcafee.com/de/products/cloud-visibility-community-edition.aspx

Rechtlicher Hinweis:

- Kundendaten, die an einen Cloud-Dienst von McAfee übertragen werden, werden unter Umständen außerhalb des Herkunftslandes gespeichert und unterliegen den **Vereinbarungen zu den Service-Bedingungen für die Intel Security-Cloud**.
- McAfee Cloud Visibility – Community Edition unterliegt ebenfalls diesen **Vereinbarungen zu den Service-Bedingungen für die Intel Security-Cloud**. Intel Security kann McAfee Cloud Visibility – Community Edition jederzeit nach eigenem Ermessen einstellen oder ändern. Weitere Hilfe finden Sie unter **www.community.mcafee.com**. Intel Security ist nicht verpflichtet, Kundendaten oder andere Informationen von Kunden aufzubewahren. Die vollständigen Bedingungen finden Sie in den **Vereinbarungen zu den Service-Bedingungen für die Intel Security-Cloud** im Abschnitt „Kostenlose Dienste“.

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