McAfee MVISION Cloud

Cloud-Sicherheit, die Ihr Geschäft ankurbelt

McAfee® MVISION Cloud schützt Daten und wehrt Bedrohungen in der Cloud in SaaS-, PaaS- und IaaS-Umgebungen mit einem einzigen Cloud-eigenen Durchsetzungspunkt ab.

Überblick

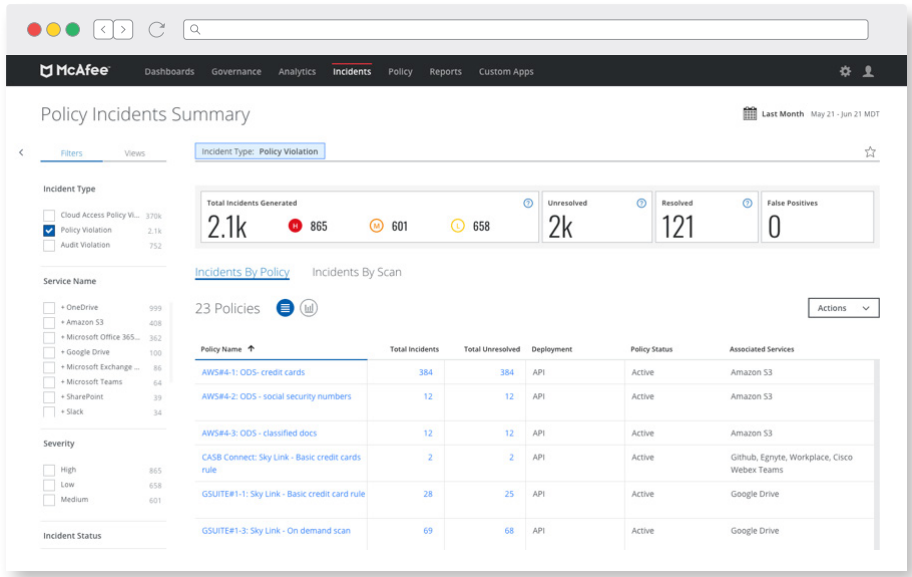
Überblick über die gesamte Cloud-Nutzung und die vorhandenen Daten

Kontrolle

Kontrolle über Daten und Cloud-Aktivitäten aus jeder beliebigen Quelle

Schutz

Schutz vor Cloud-Bedrohungen und Fehlkonfigurationen



Wichtige Anwendungsszenarien

- Mit Endgeräte-DLP synchronisierte Durchsetzung von DLP-Richtlinien (Schutz vor Datenkompromittierungen) für Daten in der Cloud
- Verhinderung von nicht autorisierter Weitergabe vertraulicher Daten an die falschen Personen
- Blockierung der Synchronisierung bzw. des Downloads von Unternehmensdaten auf private Geräte
- Erkennung von kompromittierten Konten, Insider-Bedrohungen und Malware

Folgen Sie uns

Die MVISION Cloud-Platform

Modul für einheitliche Richtlinien

Wendet einheitliche Richtlinien in allen Cloud-Diensten auf gespeicherte und übertragene Daten an. Nutzt Richtlinienvorlagen, importiert Richtlinien aus vorhandenen Lösungen und ermöglicht die Erstellung neuer Richtlinien.

Vordefinierte Richtlinienvorlagen

Enthält standardmäßig Richtlinienvorlagen basierend auf spezifischen Geschäftsanforderungen, Compliance-Vorschriften, Branche, Cloud-Dienst sowie Drittanbieter-Benchmarks.

Assistent für die Richtlinienerstellung

Definiert benutzerdefinierte Richtlinien mithilfe von Regeln, die mit boolescher Logik, Ausnahmen und mehrstufigen Behebungsmaßnahmen basierend auf dem Schweregrad von Zwischenfällen verbunden sind.

Verwaltung von Richtlinienzwischenfällen

Bietet eine einheitliche Übersicht zur Anzeige von Zwischenfällen, Durchführung manueller Aktionen sowie Zurücksetzung automatischer Behebungsaktionen zur Wiederherstellung von Dateien und ihren Berechtigungen.

Cloud-Registrierung

Bietet die weltweit größte und zuverlässigste Registrierung von Cloud-Diensten mit einer 1–10-CloudTrust-Bewertung basierend auf einer Risikobeurteilung mit 261 Punkten.

Datenschutz

Nutzt einen nicht umkehrbaren unidirektionalen Prozess zur lokalen Umwandlung aller personenbezogenen Benutzerdaten und Verschleierung der Unternehmensidentität.

Autonome Behebung

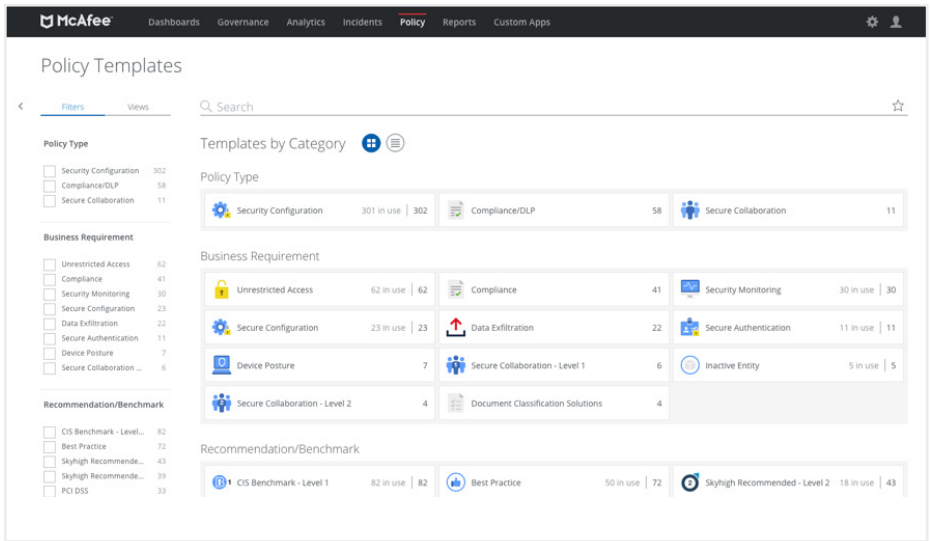
Unterstützt Benutzer bei der Behebung von Richtlinienzwischenfällen und erklärt anschließend automatisch Zwischenfallwarnungen als erledigt, sodass weniger Zwischenfälle manuell geprüft werden müssen.

In-App-Coaching

Wenn es zu einem Zwischenfall kommt, wird der Benutzer in Echtzeit in der jeweiligen E-Mail-, Messaging- und Zusammenarbeitsanwendung darüber informiert.

Wichtige Anwendungsszenarien (Fortsetzung)

- Verschlüsselung von Cloud-Daten mit Schlüsseln, auf die nur Sie allein Zugriff haben
- Überblick über nicht genehmigte Anwendungen und Kontrolle ihrer Funktionen
- Audits auf Fehlkonfigurationen anhand von Branchen-Benchmarks und automatische Änderung von Einstellungen



KI-gestützte Aktivitätszuordnung

Nutzt künstliche Intelligenz zur Analyse von Anwendungen und Zuordnung von Benutzeraktionen zu einem einheitlichen Satz von Aktivitäten, was standardisierte Überwachung und anwendungsübergreifende Kontrollen ermöglicht.

Multi-Cloud-Schutz

Erzwingt einen einheitlichen Satz von Sicherheitsrichtlinien für alle Cloud-Dienste und bietet die Möglichkeit, Richtlinienverstöße zu verknüpfen sowie Aktivitäten, Anomalien und Bedrohungen individueller Dienste zu untersuchen.

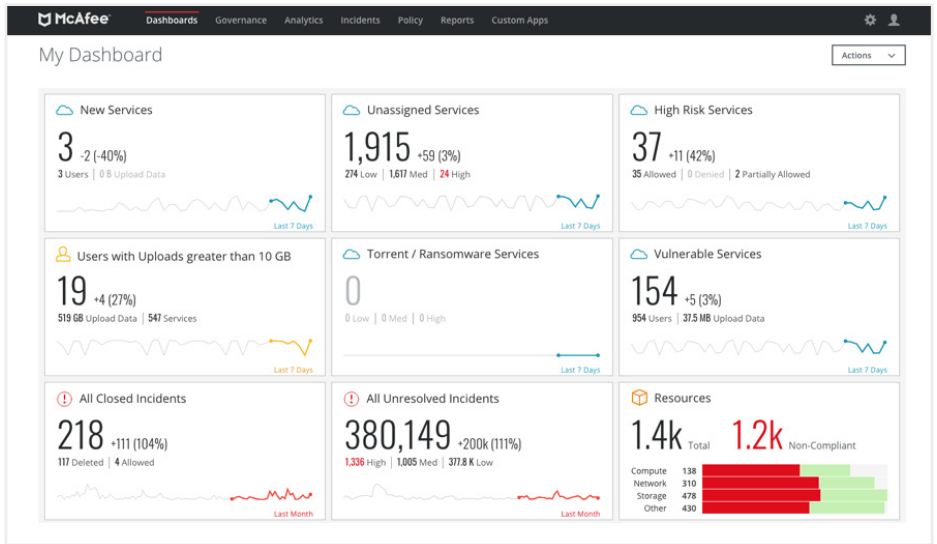
Überblick über die gesamte Cloud-Nutzung und die vorhandenen Daten

Inhaltsanalysen

Nutzt Schlüsselwörter, vordefinierte alphanumerische Muster, reguläre Ausdrücke, Datei-Metadaten und Dokument- sowie Datenbank-Fingerabdrücke, um vertrauliche Daten in Cloud-Diensten zu identifizieren.

Analyse der Zusammenarbeit

Erkennt detailliert Anzeige-, Bearbeitungs- und Eigentümerberechtigungen für Dateien und Ordner, die für einzelne Benutzer, das gesamte Unternehmen oder jeden Nutzer eines Links freigegeben sind.



„McAfee MVISION Cloud bietet Einblicke in die IT-Dienstelücke und gibt uns die Möglichkeit, Trends und Muster zu erkennen. So können wir unseren Kunden bessere Dienstleistungen anbieten und bessere Entscheidungen für unsere langfristige strategische Planung und Investitionen treffen.“

– David Stevens, Chief Information Officer, Maricopa County

Zugriffsanalysen

Erkennt den Zugriffskontext einschließlich Geräte-Betriebssystem, Geräteverwaltungsstatus, Standort sowie unternehmenseigene/private Konten.

Analyse der Cloud-Nutzung

Bietet eine Zusammenfassung der Cloud-Nutzung, einschließlich von einem Benutzer verwendete Cloud-Dienste, Datenvolumen, Upload-Zähler, Zugriffszähler sowie zugelassene/verweigerte Aktivitäten über einen Zeitraum hinweg.

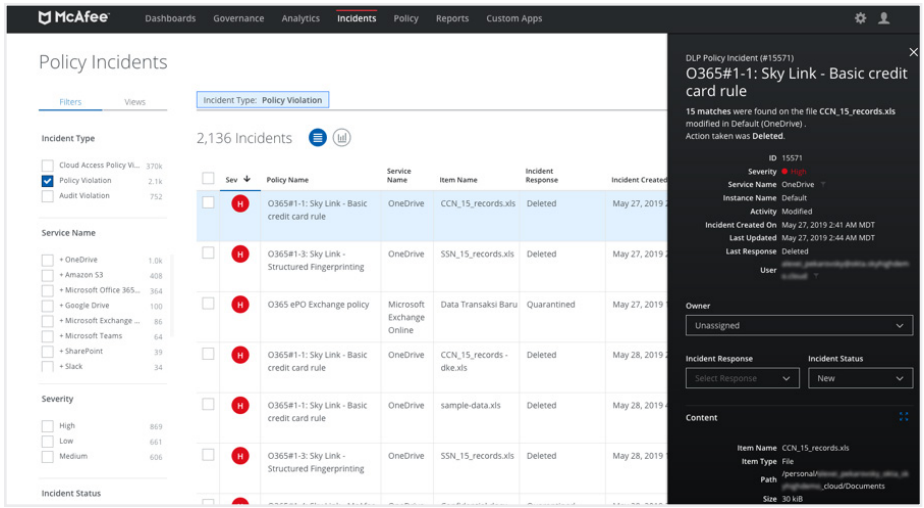
Überwachung der Cloud-Aktivitäten

Erstellt ein umfassendes Audit-Protokoll aller Benutzer- und Administrator-Aktivitäten zur Unterstützung von Untersuchungen und Forensik-Maßnahmen nach Vorfällen.

Kontrolle von Daten und Aktivitäten in der Cloud

Schutz vor Datenkompromittierung (DLP) über die Cloud

Erzwingt Richtlinien entsprechend Ihren eigenen Inhaltsregeln, um Datenkompromittierungen bei Dateien und strukturierten sowie unstrukturierten Daten in Cloud-Anwendungen und der Cloud-Infrastruktur zu verhindern. Lokale McAfee® Data Loss Prevention (DLP) Inhaltsregeln und -Richtlinien können mit MVISION Cloud synchronisiert und für Cloud-Dienste angewendet werden.



Kontrolle über mehrere Quellen

Setzt DLP-Richtlinien für Daten durch, die in die Cloud hochgeladen, in der Cloud erstellt, mit Mitarbeitern geteilt, von einem Cloud-Dienst zu einem anderen übertragen sowie aus der Cloud heruntergeladen werden.

Mehrstufige Reaktion

Definiert Richtlinien mit mehreren Schweregraden und erzwingt unterschiedliche Gegenmaßnahmen basierend auf dem Schweregrad des Zwischenfalls. Abwehrmaßnahmen wie ein DLP-Scan können bei in Audits festgestellten Fehlkonfigurationen automatisch ausgelöst werden.

„Mit McAfee können wir Sicherheitsrichtlinien wie Schutz vor Datenkompromittierung (DLP), Rechteverwaltung, Datenklassifizierung, Bedrohungsschutz und Verschlüsselung über eine zentrale Sicherheitsplattform durchsetzen, die in der Cloud und für die Cloud entwickelt wurde."

– Mauro Loda, Chief Cloud Security Architect, DuPont

Quarantäne

Isoliert Dateien, die Richtlinien ausgelöst haben, an einem sicheren Ort mit Administratorzugriff innerhalb des Cloud-Dienstes, in dem sie gefunden wurden. Die isolierten Dateien werden von McAfee niemals gespeichert.

Verschlüsselung

Schützt vertrauliche Daten mit geprüften Verschlüsselungsschemas, die vom Kunden kontrollierte Schlüssel für strukturierte sowie unstrukturierte Daten verwenden und die Funktion der Dateien beibehalten.

Information Rights Management

Bietet Rechteverwaltungsschutz für Dateien, die von Cloud-Diensten herunter- oder zu Cloud-Diensten hochgeladen wurden, damit vertrauliche Daten überall geschützt sind.

Zusammenarbeitskontrollen

Stuft Datei- und Ordnerberechtigungen bestimmter Benutzer für die Anzeige oder Bearbeitung herab, entfernt Berechtigungen und sperrt freigegebene Links. Berechtigungen können basierend auf der Vertraulichkeit der Daten festgelegt werden.

Verbundene Anwendungen

Bietet einen Überblick über Drittanbieter-Anwendungen, die mit genehmigten Cloud-Diensten wie Marktplatz-Anwendungen verbunden sind. Dadurch ist die Kontrolle von Drittanbieter-Anwendungen basierend auf bestimmten Benutzern, Anwendungen oder Zugriffsberechtigungen möglich.

Beseitigung

Entfernt Daten, die gegen Richtlinien verstoßen, dauerhaft aus Cloud-Diensten und gewährleistet damit die Einhaltung von Compliance-Vorschriften.

Kontextabhängige Zugriffssteuerung

Erzwingt allgemeine Zugriffsregeln (Gewährung/Blockierung) basierend auf den Risiken des jeweiligen Dienstes, dem Gerätetyp sowie auf detaillierten Aktivitätskontrollen. So wird das Hoch- und Herunterladen von Daten verhindert.

Adaptive Authentifizierung

Erzwingt in Echtzeit zusätzliche Authentifizierungsschritte. Dazu werden Identitätsverwaltungslösungen basierend auf Richtlinien für Zugriffskontrolle integriert.

Kontrolle über Cloud-Anwendungen

Bietet detaillierte Richtlinien für nicht genehmigte Cloud-Dienste einschließlich der Möglichkeit zum Zulassen oder Blockieren von Aktivitäten sowie Zugriffskontrolle auf nicht genehmigte Mandanten über die MVISION Cloud-Konsole.

Schutz vor Cloud-Bedrohungen und Fehlkonfigurationen

Überprüfung der Sicherheitskonfiguration

Erkennt aktuelle Sicherheitseinstellungen für Cloud-Anwendungen oder die Infrastruktur und schlägt Veränderungen vor, die die Sicherheit entsprechend Branchenempfehlungen wie den CIS-Benchmarks (Center for Internet Security) verbessern. Vor der Bereitstellung von Code in der IaaS-Umgebung (Infrastructure-as-a-Service) können Audits durchgeführt werden, um die Risiken präventiv zu minimieren.

Automatisierte Behebung von Konfigurationsfehlern

Ermöglicht eine richtlinienbasierte Reaktion auf Fehlkonfigurationen, die bei einem Audit entdeckt wurden. Dabei wird die Einstellung automatisch geändert (z. B. öffentlicher Zugriff auf einen IaaS-Storage-Bucket deaktiviert).

Verhaltensanalyse von Benutzern und Entitäten (UEBA)

Erstellt automatisch ein selbstlernendes Modell basierend auf mehreren Heuristiken sowie Machine Learning und erkennt über mehrere Cloud-Dienste Aktivitätsmuster, die auf Benutzerbedrohungen hinweisen.

Geführtes Machine Learning

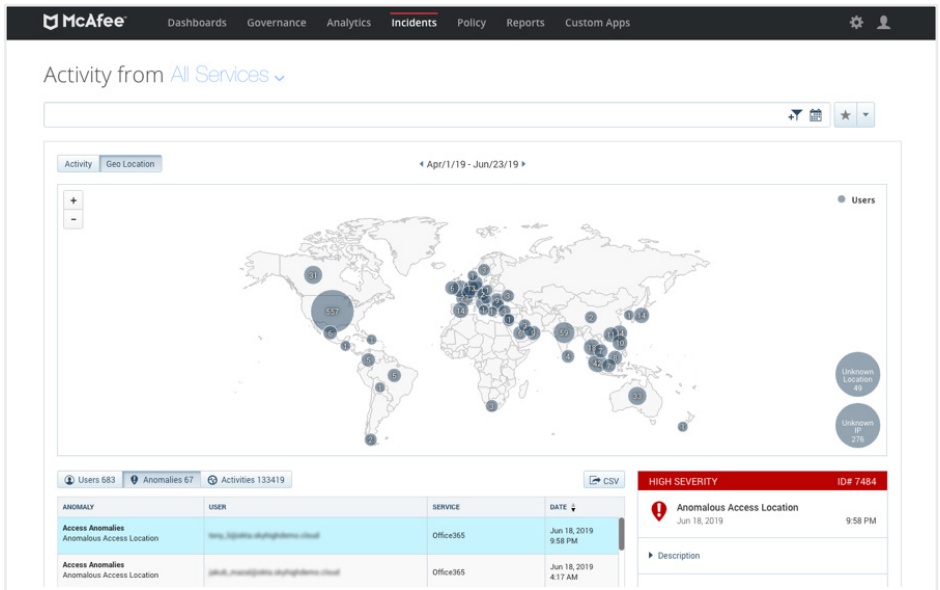
Ermöglicht menschlichen Einfluss auf Machine Learning-Modelle mit Echtzeit-Vorschau der Auswirkungen von Empfindlichkeitsänderungen auf Anomalien, die im System entdeckt wurden.

Erkennung von Kontenkompromittierung

Analysiert Anmeldeversuche zur Erkennung unmöglicher regionsübergreifender Zugriffe, Brute-Force-Angriffe sowie nicht vertrauenswürdiger Standorte, die auf kompromittierte Konten hinweisen.

Erkennung von Insider-Bedrohungen

Nutzt Machine Learning zur Erkennung von Aktivitäten, die auf fahrlässiges und böswilliges Verhalten (z. B. Diebstahl vertraulicher Daten) hinweisen.



Analysen privilegierter Benutzer

Erkennt zu weit gefasste Benutzerberechtigungen, inaktive Konten, nicht genehmigte Zugriffe und unbefugte Eskalation von Berechtigungen sowie Benutzerbereitstellungen.

Malware-Erkennung

Erkennt Malware und deckt Verhalten auf, das auf Malware hinweist, die Daten aus Cloud-Diensten exfiltriert. Cloud-Dienste können auf Abruf auf vorangegangene Kompromittierungen und in Echtzeit gescannt werden.

Malware-Entfernung

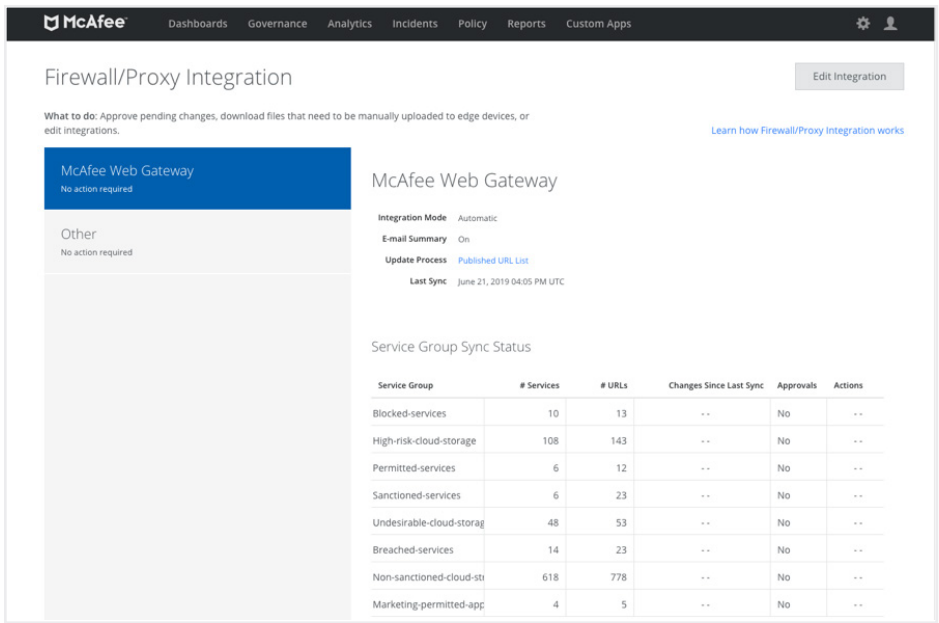
Beseitigt hochentwickelte Bedrohungen durch die dauerhafte Neutralisierung und Entfernung von Malware.

„Dank McAfee verstehen wir, wie unsere Mitarbeiter Salesforce nutzen. Dadurch können wir Insider-Bedrohungen, kompromittierte Anmeldeinformationen sowie zu weit gefasste Benutzerberechtigungen aufdecken."

– Mike Bartholomy, Senior Manager, Information Security, Western Union

Integrierte Unternehmenstechnologien

- Schutz vor Datenkompromittierungen (DLP)
- Sicherheitsinformations- und Ereignis-Management (SIEM)
- Sicheres Web-Gateway (SWG)
- Firewall der nächsten Generation (NGFW)
- Schlüsselverwaltungsdienst (KMS)
- Identitäts- und Zugriffsverwaltung (IAM)
- Information Rights Management (IRM)
- Enterprise Mobility Management (EMM/MDM)
- Verzeichnisdienste (LDAP)



Bereitstellungsvarianten

McAfee Sky Link

Verbindet sich mit den APIs von Cloud-Diensten, um einen Überblick über die Daten und Benutzeraktivitäten zu erhalten sowie nahezu in Echtzeit Richtlinien für hochgeladene, freigegebene und gespeicherte Daten durchzusetzen.

McAfee Lightning Link

Richtet eine direkte Out-of-Band-Verbindung zu Cloud-Diensten ein, um in Echtzeit Richtlinien für Daten, Benutzer und Geräte umfassend zu erzwingen.

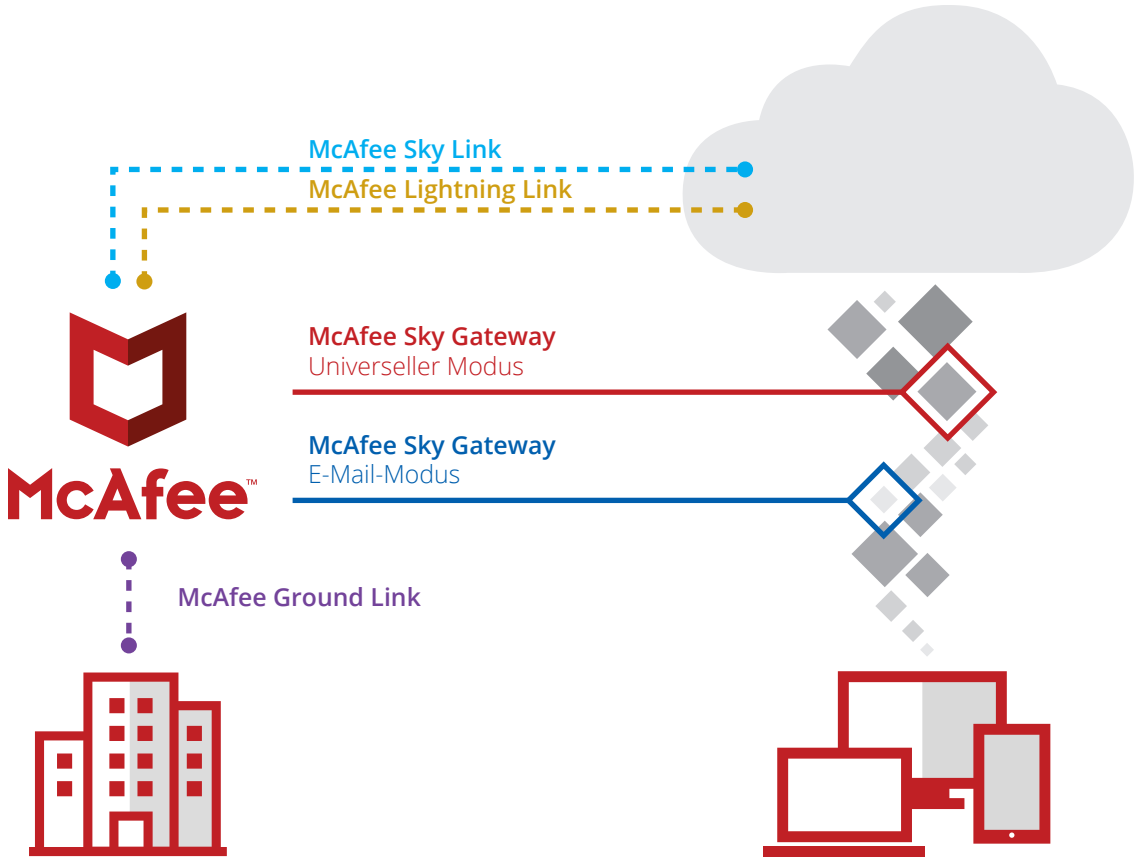
McAfee Ground Link

Richtet eine Verbindung zwischen McAfee und lokalen LDAP-Verzeichnisdiensten, DLP-Lösungen, Proxys, Firewalls und Schlüsselverwaltungsdiensten ein.

McAfee Sky Gateway

Setzt Richtlinien für übertragene Daten in Echtzeit inline durch.

- **E-Mail-Modus:** Nutzt den systemeigenen E-Mail-Fluss zur Durchsetzung von Richtlinien für alle Nachrichten, die von Exchange Online gesendet wurden, inline oder im passiven Überwachungsmodus.
- **Universeller Modus:** Setzt inline zwischen Benutzer und Cloud-Dienst an und steuert den Datenverkehr nach der Authentifizierung, um auch ohne Agenten alle Benutzer und alle Geräte abzudecken.

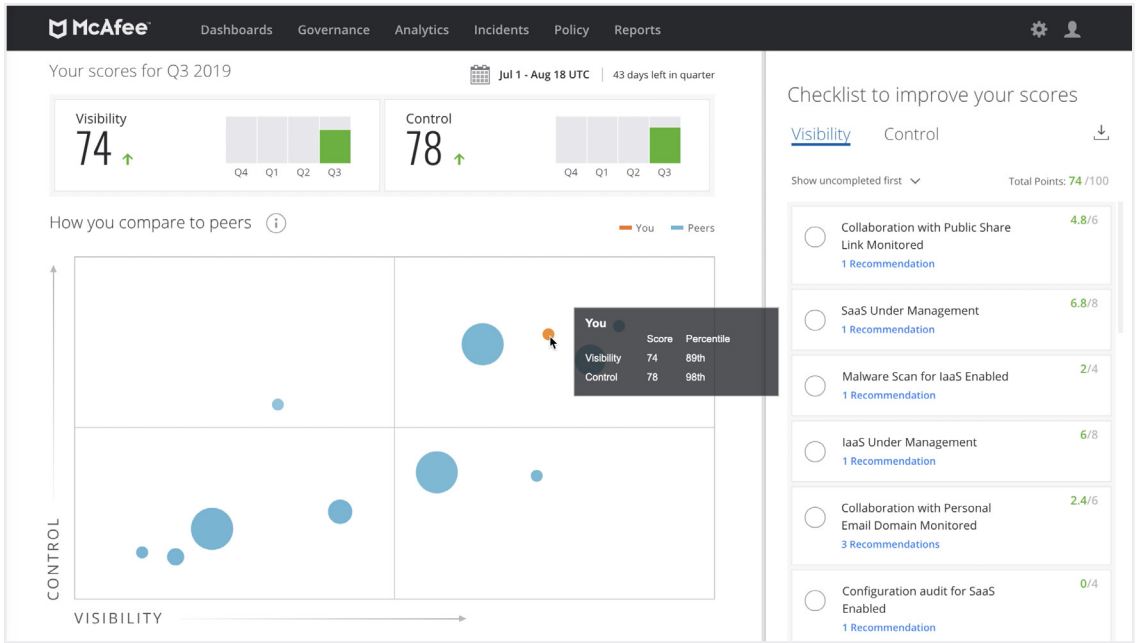


Cloud Security Advisor

Cloud Security Advisor ist ein Portal in der MVISION Cloud Security-Plattform, mit dem Kunden ihren Cloud-Sicherheitsprozess überwachen können. Es gibt Unternehmen einzigartige Empfehlungen dazu, wie diese ihre Maßnahmen zur Implementierung von Cloud-Sicherheitskontrollen priorisieren können.

Cloud Security Advisor bietet:

- **Bericht zur Cloud-Sicherheit:** Ein Überblick über wichtige Nutzungsstatistiken zu wichtigen Sicherheitskennzahlen wie Cloud-Nutzung, Zwischenfälle, gefährdete Daten und Anzahl der Benutzer.
- **Cloud Security Advisor-Bewertung und Quadrant:** Bietet Bewertungen der Übersicht und Kontrolle jeweils auf einer Skala von 1 bis 100. Die Werte basieren auf Cloud-Sicherheitskennzahlen sowie dem Implementierungsfortschritt und werden mit Branchenvertretern (ähnlicher Größe) verglichen.
- **Empfehlungen zur Cloud-Sicherheit:** Stellt Unternehmen einzigartige präskriptive Empfehlungen in der Reihenfolge ihrer Priorität bereit, um die Cloud-Sicherheit zu verbessern. Die Empfehlungen werden nach Punkten entsprechend ihrer potenziellen Auswirkungen gewichtet.

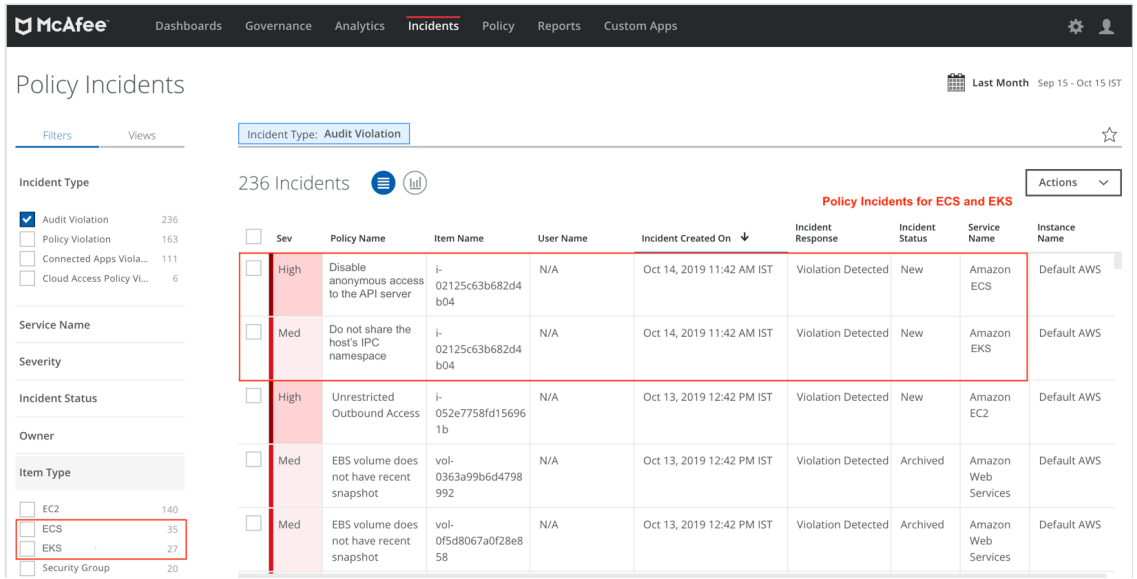


MVISION Cloud for Containers

Container-Workloads sind die natürliche Folge von Virtualisierung und sind optimiert, um die Vorteile der Cloud bestmöglich nutzen zu können. MVISION Cloud Container Security bietet eine einheitliche Cloud-Sicherheitsplattform mit für Container optimierten Strategien zur Absicherung dynamischer und wandlungsfähiger Container-Workloads sowie der zugrunde liegenden Infrastruktur.

MVISION Cloud for Containers bietet:

- **Schwachstellenanalyse** für Container-Komponenten
  - Bewertet den in Container eingebetteten Code zum Erstellungszeitpunkt sowie in Intervallen, damit gewährleistet ist, dass bekannte Risiken aufgedeckt oder minimiert werden und somit böswillige Akteure weniger Möglichkeiten haben, in einen Container-Workload zu gelangen.
- **Verwaltung der Cloud-Sicherheitslage** für Container-Infrastrukturen und Koordinierungssysteme wie Kubernetes
  - Gewährleistet, dass die Konfiguration der Umgebung keine Risiken entstehen lässt.
  - Gewährleistet, dass sich die Konfiguration der Umgebung nicht im Laufe der Zeit verändert und zu unerwünschten Risiken führt.
- **Nano-Segmentierung** für die Kommunikation zwischen Containern
  - Zero Trust: Stets überprüfen, niemals vertrauen. Erkennt und überwacht das Verhalten der Netzwerkkommunikation zwischen Container-Prozessen, trägt dabei der Wandlungsfähigkeit von Containern Rechnung und benötigt keine externen Faktoren wie eine IP-Adresse.



- Erkennt ungewöhnliche Kommunikation und meldet oder blockiert sie je nach Benutzereinstellung.
- Erkennt Veränderungen bei Kommunikationsmustern zwischen Container-Versionen im Laufe der Anwendung.
- Nutzt bekannt gute Konfigurationen zur Absicherung von Workloads, anstatt ständig nach bekannt schlechten zu suchen.

McAfee
Together is power.

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