McAfee Unified Cloud Edge

Datensicherheit vom Gerät bis zur Cloud und Abwehr unsichtbarer Cloud-nativer Bedrohungen im Unternehmensnetzwerk

Mehr als 95 % der Unternehmen nutzen heute bereits Cloud-Dienste und 83 % speichern vertrauliche Daten in der Cloud.[1] Mit Mobilgeräten und Laptops können Mitarbeiter innerhalb und außerhalb des Unternehmensnetzwerks arbeiten. Dadurch vergrößert sich der zu schützende Bereich bis zu einer neuen von der Cloud definierten Grenze. Dennoch können heute nur 30 % der Unternehmen Daten mithilfe identischer Richtlinien auf ihren Geräten, im Netzwerk und in der Cloud schützen. Nur 36 % können überhaupt Regeln für den Schutz vor Datenkompromittierungen (DLP) in der Cloud durchsetzen. 60 % haben momentan keine Möglichkeit, ein ungesichertes privates Mobilgerät davon abzuhalten, komplett unsichtbar für die IT vertrauliche Daten aus der Cloud herunterzuladen.[2] Weil immer mehr Daten zwischen Geräten und der Cloud bzw. zwischen Clouds übertragen werden, brauchen Unternehmen eine neue Methode für die konsistente Absicherung ihrer Daten. Das ist McAfee® Unified Cloud Edge.

Folgen Sie uns

McAfee Unified Cloud Edge

McAfee Unified Cloud Edge ist Bestandteil von McAfee® MVISION, der Cloud-nativen Sicherheitsplattform von McAfee. McAfee Unified Cloud Edge bietet durchgehende Kontrollen für Datensicherheit und Bedrohungsschutz vom Gerät bis zur Cloud. Das Produkt basiert auf drei Kerntechnologien, die zu einer Lösung vereint wurden:

1. **Cloud Access Security Broker (CASB):** Transparenz und Kontrolle für Cloud-Dienste durch direkte API-Verbindung und Reverse Proxy
2. **Sicheres Web-Gateway (SWG):** Proxy-basierte Transparenz und Kontrolle für Web-Datenverkehr und nicht genehmigte Cloud-Dienste
3. **Schutz vor Datenkompromittierungen (DLP):** Agenten- und netzwerkbasierte Transparenz und Kontrolle für sensible Daten

Diese Technologien arbeiten zusammen, um Daten vom Gerät bis zur Cloud zu schützen und Cloud-interne Kompromittierungsversuche abzuwehren, die im Unternehmensnetzwerk nicht sichtbar sind. Sie schaffen eine sichere Umgebung für die Nutzung der Cloud-Dienste und ermöglichen den Cloud-Zugriff von jedem Gerät aus. Dies bedeutet maximale Produktivität für alle Mitarbeiter. Unternehmen können durch die schnelle Implementierung transformativer Cloud-Dienste erfolgreicher agieren, indem sie ihre Daten und Ressourcen mit McAfee Unified Cloud Edge schützen.

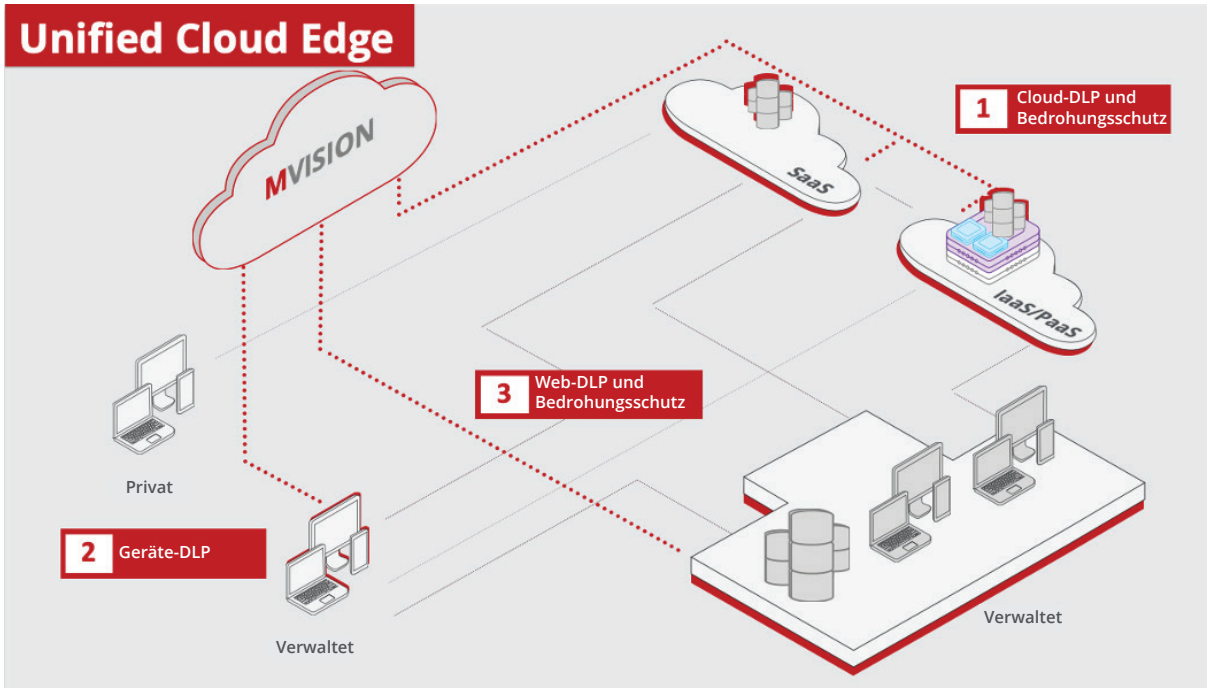

Abbildung 1. Vereinfachte Architektur für McAfee Unified Cloud Edge.

Einfachere und schnellere Prozesse durch Konvergenz

Der individuelle Betrieb dieser Technologien würde ein komplexes Management erfordern. Alle drei nutzen DLP am Endgerät, im Netzwerk oder in der Cloud, sodass bei einer separaten Verwaltung ein enormer Zusatzaufwand entstehen würde. Die Untersuchung von Sicherheitsereignissen in diesem Spektrum würde bedeuten, dass die Berichte einzelner Produkte und Repositorys manuell zusammengefügt werden müssten, um den Weg der Daten von einem Gerät in die Cloud (bzw. oft auch zu einem externen Ziel) verfolgen zu können. Die Kontrolle über den Zugriff auf Cloud-Dienste verteilt sich ineffizient auf Web-Proxys und Cloud Access Security Broker, die jeweils individuelle Zugriffsrichtlinien implementieren. Aktuelle Architekturen sind Hardware-limitiert, sodass Netzwerkkosten und Kapazitätsgrenzen dem Potenzial der Cloud Grenzen setzen.

Konvergenz bedeutet Einfachheit. Mit McAfee Unified Cloud Edge können Sie folgende Ziele erreichen:

- Konsistente Transparenz und durchgehende Kontrolle der Datenübertragung vom Gerät bis zur Cloud
- Einheitliche Zugriffssteuerungs- und Bedrohungsschutz-Funktionen für Cloud und Web
- Cloud-native und Direct-to-Cloud-Architektur mit unternehmensgerechter Skalierung und Resilienz

Unsere Arbeit verlagert sich immer mehr vom Netzwerk in die Cloud. Mit McAfee Unified Cloud Edge können Ihre Mitarbeiter maximal produktiv arbeiten, während Sie gleichzeitig von effizientem und einheitlichem Sicherheitsmanagement mit Cloud-Geschwindigkeit profitieren.

Umfassende Transparenz und durchgehende Kontrolle der Datenübertragung vom Gerät bis zur Cloud

Der Wechsel in die Cloud bedeutet, dass immer mehr Daten vom Netzwerk in die Umgebungen der Cloud-Anbieter verlagert werden. Dadurch verschieben sich auch die primären Kontrollpunkte für die Datensicherheit. Geräte können von überall auf Cloud-Daten zugreifen, und Daten können in der Cloud erstellt oder von verschiedenen Clouds genutzt werden, ohne jemals auf einem Gerät zu landen. Damit sind Gerät und Cloud wichtige Punkte für die Datensicherheit. Der Web-Datenverkehr im Netzwerk bleibt hingegen eine nützliche Methode, um nicht genehmigte Cloud-Dienste zu kontrollieren, Malware zu verhindern und den allgemeinen Internet-Zugriff zu verwalten.

Viele Unternehmen nutzen DLP bereits erfolgreich in ihren lokalen Umgebungen und haben in Zusammenarbeit mit Rechtsabteilung, Marketing, Kunden-Support und nahezu allen anderen Abteilungen viel Zeit in die Klassifizierung der sensiblen Daten für ihr Unternehmen investiert, um alle Datenschutzanforderungen zu erfassen.

Die Implementierung von DLP in der Cloud erforderte bislang einen Neuaufbau dieser DLP-Klassifizierungen für die Cloud. Dies führte zu enormem Zeitaufwand für die Replikation von Arbeitsschritten, 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 Zusammenarbeits-Tools oder freigegebene Links in der Cloud nicht erkennen.

McAfee Unified Cloud Edge erleichtert die DLP-Implementierung in der Cloud, indem Datenklassifizierungen und DLP-Module für alle Durchsetzungspunkte genutzt werden: Gerät, Netzwerk und Cloud. Sobald Klassifizierungen mit McAfee® ePolicy Orchestrator® (McAfee ePO™) erstellt und organisiert wurden, können Sie sie zwischen dem lokalen DLP und CASB synchronisieren. Sie werden dabei auf die Richtlinien für jeden Cloud-Dienst und jeden Verkehr zwischen Clouds angewendet, der Ihr Netzwerk ansonsten umgehen würde. Alle Geräte innerhalb oder außerhalb Ihres verwalteten Netzwerks können durch dieselben DLP-Regeln geschützt werden.

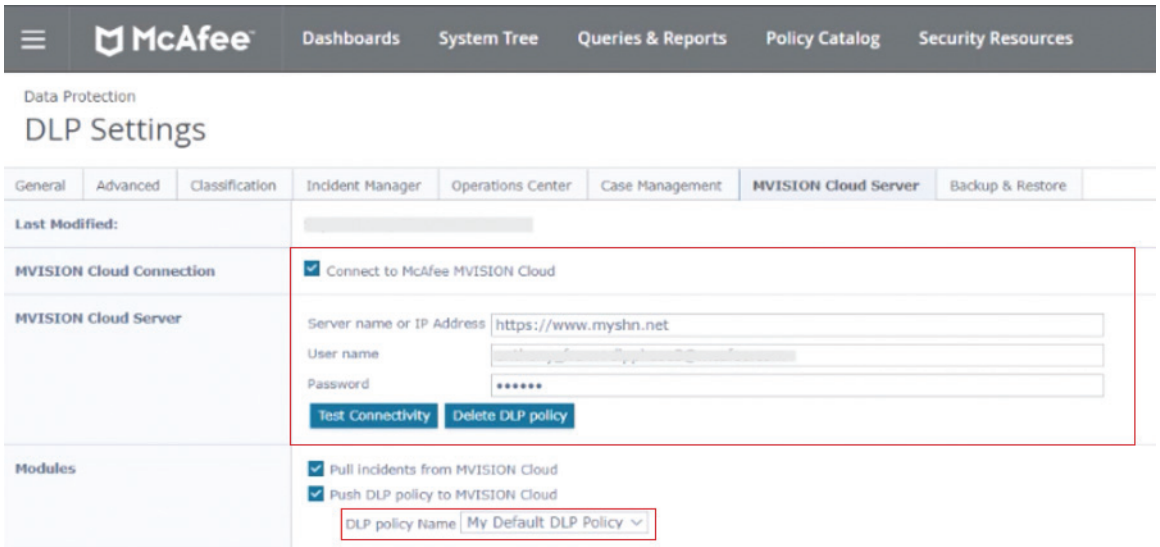

Abbildung 2. Übermittlung der DLP-Klassifizierungen im Push-Verfahren von McAfee ePO zum CASB.

Unternehmen, die die Datensicherheit für Endgeräte, das Netzwerk und die Cloud separat verwalten, müssen mit einer komplexen Konfiguration arbeiten, bei denen sich die alltäglichen Aufgaben wie die Verwaltung von Zwischenfällen, Untersuchungen und Berichte an verschiedenen Stellen befinden. Das Zusammenfügen dieser Informationen zu einem umfassenden Überblick vom Gerät bis zur Cloud ist zeitaufwändig. Zudem lässt sich kaum genau arbeiten, und oft ist es schlicht unmöglich, Kompromittierungsvorfälle von Anfang bis Ende zu verfolgen, da auf jedem Kontrollpunkt nach anderen Spuren gesucht werden muss.

McAfee Unified Cloud Edge löst dieses Problem, weil damit die Verwaltung von Zwischenfällen, die Workflows für Untersuchungen und die Berichte an einer Stelle vereint werden. Alle drei Durchsetzungspunkte – Gerät, Netzwerk und Cloud – übertragen ihre Ereignisdaten an einen Ort und nutzen auch dieselben DLP-Module und Klassifizierungen. Dieser zentrale Ort ist die Software McAfee ePO, die die Erstellung der Datenklassifizierung und die Ergebnisse ihrer Richtlinienimplementierung zusammenführt.

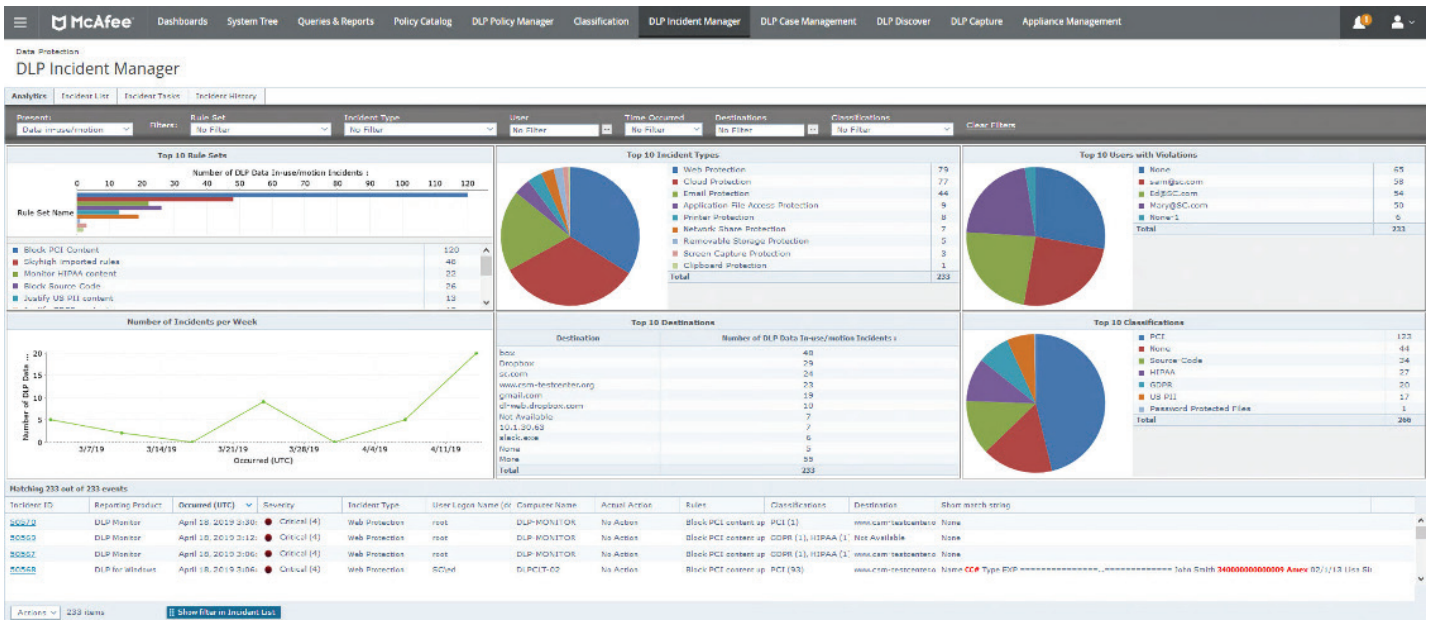

Abbildung 3. Einheitliche DLP-Berichte für Geräte, Netzwerk und Cloud in McAfee ePO.

Die zentrale DLP-Verwaltung spart Zeit, weil sie schnellere Untersuchungen und Berichte ermöglicht, ohne dass mehrere Datenquellen kombiniert werden müssen. Die Untersuchungen und Berichte sind zuverlässiger und weniger anfällig für Fehler durch die manuelle Kombination von Daten. Stattdessen werden die Daten von McAfee ePO automatisch zusammengeführt. Die Zwischenfalldaten sind vollständig und konsistent, verwenden dieselben DLP-Module und Klassifizierungen für jeden Durchsetzungspunkt und kombinieren ihre Ereignisdaten.

Einheitliche Zugriffssteuerungs- und Bedrohungsschutz-Funktionen für Cloud und Web

Cloud-Dienste weisen mehrere Risikostufen auf. Gleichzeitig ist der Zugriff sowohl über verwaltete als auch private Geräte möglich. Unternehmens-Cloud-Dienste wie Microsoft Office 365 haben Anwendungsprogrammierschnittstellen (APIs) veröffentlicht, mit denen sich CASBs direkt verbinden können. Dies gewährleistet die Transparenz und Kontrolle für Daten, die in den Dienst einfließen sowie in der Cloud erstellt, zwischen den Clouds ausgetauscht oder extern genutzt werden. Cloud-interne Bedrohungen in diesen Diensten können durch Verhaltensanalysen von Benutzern und Entitäten (UEBAs) erkannt werden. Sie korrelieren die Aktivitäten aus allen verwendeten Cloud-Diensten. Private Geräte können z. B. versuchen, auf Unternehmensinstanzen von Office 365 zuzugreifen, und vom CASB für das Herunterladen von Daten blockiert werden.

Die meisten Unternehmen gehen davon aus, dass sie nur 35 Dienste verwenden – in Wirklichkeit sind es aber eher 2.000.[3] Das ist eine große Anzahl von Diensten, die geschützt werden müssen. 90 % der Daten entfallen auf die Unternehmensdienste, die von der IT genehmigt wurden, 42 % allein auf Zusammenarbeitsdienste wie Office 365. Die verbleibenden 10 % der Daten entfallen auf nicht genehmigte Dienste, die häufig als „Schatten-IT“ bezeichnet werden.[4] Obwohl sich darunter nur wenige vertrauliche Daten befinden, stellen sie in der Regel in höheres Risiko dar, weil sie bestimmte Sicherheitsanforderungen nicht erfüllen, z. B. weil gespeicherte Daten nicht verschlüsselt werden oder die Dienste keine Compliance-Zertifizierung vorweisen können.

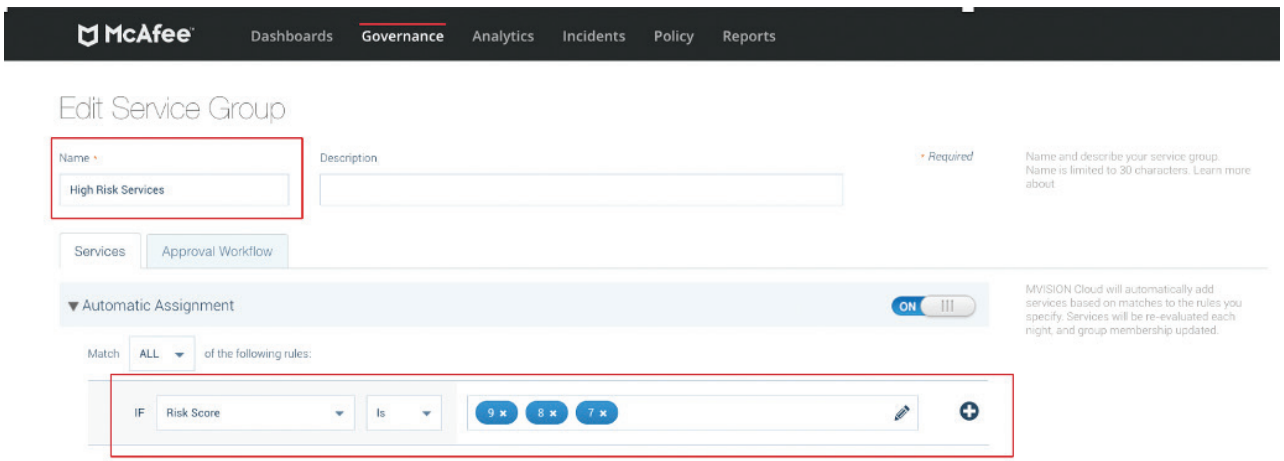

Abbildung 4. Konvergierte Cloud- und Web-Richtlinien blockieren den Web-Zugriff aller hochriskanten Cloud-Dienste.

Mit McAfee Unified Cloud Edge können Sie über eine einzige Konsole den Zugriff auf alle Cloud-Dienste steuern und diese Dienste vor Bedrohungen schützen. In dieser Konsole haben Sie Zugriff auf den McAfee-CASB und das Cloud-native SWG, die zu Richtlinien für eine bisher unerreichte Cloud-Kontrolle kombiniert werden können. Abbildung 4 zeigt ein Richtlinienbeispiel, das alle aktuellen und zukünftigen hochriskanten Cloud-Dienste zu einer Gruppe zusammenfasst, die zur Beschränkung des Web-Zugriffs verwendet werden kann. Dadurch werden besonders riskante Cloud-Dienste vom Cloud-nativen SWG blockiert, um Zugriffe von Endbenutzern auf diese Dienste zu verhindern und vor versehentlichen Datenverlusten und Malware-Infektionen zu schützen.

Zu den zusätzlichen Kontrollen, die sich aus der Konvergenz des CASB und SWG in McAfee Unified Cloud Edge ergeben, gehören:

- **Abwehr von Zero-Day-Malware:** Unser hocheffizientes Machine-Learning-basiertes Modul erkennt und entfernt Zero-Day-Malware aus allen Cloud-Diensten oder Webseiten.
- **Remote-Browser-Isolierung:** Schützen Sie sich umfassend davor, dass Elemente einer Webseite ein Endgerät erreichen, indem Sie Browser-Sitzungen in einer virtuellen Remote-Umgebung isolieren.
- **Kontrolle über Cloud-Anwendungen:** Kontrollieren Sie Funktionen einzelner Cloud-Dienste, z. B. das Veröffentlichen oder Hochladen von Dokumenten.
- **Mandantenbezogene Einschränkungen:** Unterscheiden Sie bei Cloud-Diensten wie Office 365 zwischen privaten und Unternehmenskonten, indem Sie private Konten blockieren und die Benutzer zu von Ihnen kontrollierten Unternehmenskonten leiten.

McAfee Unified Cloud Edge nutzt einen CASB, um die Transparenz und Kontrolle für die genehmigten Cloud-Dienste per API und Reverse Proxy zu implementieren. Für nicht genehmigte Cloud-Dienste und das Web verwendet die Lösung ein Cloud-natives SWG, um ihre Richtlinien über einen Forward Proxy durchzusetzen. Der Cloud-Zugriff und die Bedrohungen werden mit einer einzigen Cloud-nativen Benutzeroberfläche kontrolliert.

Cloud-native und Direct-to-Cloud-Architektur mit unternehmensgerechter Skalierung und Resilienz

Das netzwerkorientierte Sicherheitsmodell bietet keine adäquate Transparenz und Kontrolle mehr für Geräte, die sich überall befinden können, und Cloud-Dienste, die nicht vom Unternehmen betrieben werden. Der Zugriff von den Geräten auf die Cloud erfolgt über Web-Protokolle, die einen Kontroll-Layer für Web-Proxys bereitstellen, um Richtlinien für nicht genehmigte Dienste durchzusetzen, nach vertraulichen übertragenen Daten zu suchen und Malware zu blockieren. Viele Unternehmen nutzen heute Hardware-Appliance-Proxys in ihren Rechenzentren, die den Verkehr von Remote-Standorten mithilfe von Wide-Area-Network-Technologie wie Multiprotocol Label Switching (MPLS) erfassen. Die Hardware und das MPLS-Netzwerk sind jedoch mit Kosten sowie mit Kapazitätsgrenzen verbunden. Mit einer Cloud-nativen Architektur können die Kosten für die Hardware und das MPLS-Routing eliminiert und die Kapazitätsbeschränkungen durch die Skalierung der Cloud aufgehoben werden.

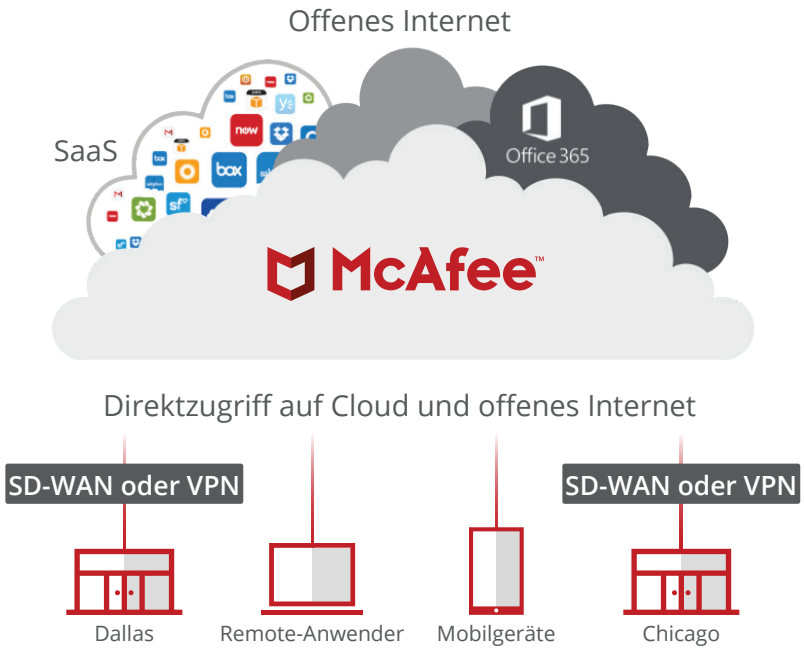

Abbildung 5. Vereinfachte Cloud-native Architektur für Web- und Cloud-Sicherheit.

Durch McAfee Unified Cloud Edge können sich jetzt alle Geräte oder physischen Standorte direkt mit der Cloud und dem offenen Internet verbinden und Daten sowie Bedrohungen besser kontrollieren. MPLS-Netzwerke sind dagegen nicht mehr erforderlich. Stattdessen regeln jetzt Software-definierte WAN- (SD-WAN-) oder VPN-Technologien den Datenverkehr von physischen Standorten in die Cloud. Andere Cloud-native Proxys bieten nicht die konvergierte kontextbezogene Kontrolle eines CASB und verursachen enorme Unterbrechungen durch ausfallende Dienste, die den Internet-Zugang verlieren. McAfee Unified Cloud Edge hat eine Dienstverfügbarkeit von 99,999 %. Dies bedeutet minimale Ausfallzeiten für Ihr Unternehmen. Ihre Architektur ist kosteneffektiv, ausfallsicher sowie aktuell und kann Daten schützen sowie Bedrohungen in der Cloud-First-Welt abwehren.

Nächste Schritte

McAfee Unified Cloud Edge kann eine einheitliche Daten- und Bedrohungskontrolle vom Gerät bis zur Cloud gewährleisten, sodass Ihr Unternehmen mit Cloud-Geschwindigkeit arbeiten kann, ohne die Transparenz und Kontrolle zu verlieren. Wenden Sie sich an McAfee, um Möglichkeiten zur Implementierung von McAfee Unified Cloud Edge in Ihrem Unternehmen zu erörtern.

- McAfee-Demo erhalten
- Produktdetails

Weitere Informationen

Weitere Informationen erhalten Sie unter **www.mcafee.com/de**.

1. McAfee (2018): Bericht zu Cloud-Nutzung und Risiken.
2. McAfee (2020): Unternehmen als Supernova: Risiken durch die Verbreitung von Daten in der Cloud.
3. McAfee (2018): Bericht zu Cloud-Nutzung und Risiken.
4. McAfee (2019): Bericht zu Cloud-Nutzung und Risiken: Ausgabe zu Unternehmenswachstum.

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