McAfee Web Gateway Cloud Service

Cloud-native Web-Sicherheit mit allgegenwärtigem Schutz

Die Abwehr raffinierter Web-Bedrohungen erfordert hochentwickelte Technologien, muss jedoch nicht zwangsläufig mehr Kosten und Komplexität bedeuten. Durch die Implementierung von Web-Sicherheit über die Cloud erzielen Sicherheitsteams denselben erweiterten Bedrohungsschutz wie mit lokalen Appliances, sparen allerdings Hardware-Kosten und Wartungsressourcen. Da der Web-Zugriff zunehmend außerhalb der Netzwerkperipherie stattfindet, wird die Cloud zum dauerhaften Kontaktpunkt für mobile Geräte und Benutzer. Statt Sicherheitskonzepte für Datenverkehr zu einem einzelnen Standort zu entwickeln, ist es effektiver, den Schutz vom jeweiligen Endgerät ausgehend aufzubauen. Durch die Vereinheitlichung von Zugriffssteuerung und Bedrohungsschutz für Cloud und Web können Ihre Mitarbeiter die Produktivität maximieren und die Sicherheitsverwaltung effizienter und konsistenter gestalten.

Kosteneffektiver, allgegenwärtiger Schutz

Die Verwaltung lokaler Web-Sicherheits-Appliances ist teuer und belastet die ohnehin schon angespannten Ressourcen der Sicherheitsteams zusätzlich.
Die Implementierung der Web-Sicherheit als Cloud-Dienst kann die Gesamtbetriebskosten senken, da keine Hardware-Appliances mehr angeschafft, betrieben und gewartet werden müssen. Alle Ressourcen, die zuvor in die Wartung der Appliances flossen (z. B. für Software-Upgrades und Patches), können nun auf strategischere Initiativen innerhalb der IT oder IT-Sicherheit gerichtet werden.

Appliances und Cloud-Dienste können zusammen in einer hybriden Implementierung genutzt werden. Die meisten Unternehmen entscheiden sich für dieses Modell, da sie so die Zuständigkeit für und Kontrolle über die Appliances im Netzwerk behalten und gleichzeitig den Cloud-basierten Schutz auf kleine externe Niederlassungen und mobile Benutzer ausdehnen können.

Wichtige Vorteile

- Kosteneffektivste Methode für die Implementierung von Web-Sicherheit – keine lokale Hard- oder Software erforderlich
- Mehr als nur Basisschutz – Verhaltensemulation wehrt Zero-Day-Malware während der Verarbeitung des Datenverkehrs innerhalb von Millisekunden ab
- Schutz für Benutzer auch außerhalb des Netzwerks – Cloud-Übertragung hebt Grenzen traditioneller Netzwerke auf
- Vereinheitlichung mit der McAfee® MVISION Cloud (CASB)-Konsole für effiziente und konsistente Sicherheitsverwaltung

Folgen Sie uns:

IT-Teams, die den Web-Datenverkehr externer Niederlassungen über MPLS-Schaltungen (MultiProtocol Label Switching) leiten (Backhauling) und durch eine Web-Gateway-Appliance im Netzwerk filtern lassen, profitieren unmittelbar von Cloud-basierter Web-Sicherheit. Backhauling ist teuer und erhöht die Komplexität im Netzwerk. Alternativ können externe Niederlassungen ihren Datenverkehr für den Schutz direkt in die Cloud leiten. Damit können MPLS-Schaltungen minimiert und die Netzwerkarchitektur vereinfacht werden.

Zudem entfällt die Beschränkung, dass Mitarbeiter nur innerhalb der Netzwerkperipherie Web-Zugriff haben und Benutzer sowie Geräte außerhalb des Netzwerks ohne Schutz und für die IT nicht sichtbar sind. Die Verlagerung der Web-Sicherheit in die Cloud invertiert diese Peripherie. Web-Datenverkehr von Benutzern und Geräten außerhalb des Netzwerks kann automatisch vom Endgerät in die Cloud geleitet werden. Dies gewährleistet Benutzern eine sichere Verbindung bei der Arbeit von zu Hause, am Flughafen, im Café oder an anderen netzwerkexternen Standorten. Das Netzwerk ist nicht mehr auf den Datenverkehr innerhalb physikalischer Grenzen beschränkt, sondern wird stattdessen vom jeweiligen Endgerät aus aufgebaut.

Globale Hochleistungsarchitektur

McAfee® Web Gateway Cloud Service wurde für Unternehmen konzipiert. Viele Firmen erzielen damit bessere Leistungswerte als mit ihrer aktuellen lokalen Lösung. Wenn beispielsweise lokale Kapazitäten ausgebaut werden müssen, ist es Aufgabe der IT-Abteilung, eine neue Appliance zu beschaffen und bereitzustellen. Dies kann Tage oder gar Wochen dauern. Aufgrund der elastischen Struktur unserer Cloud, die in den Service integriert wurde, dauern Kapazitätserweiterungen nur etwa 15 Minuten.

Wenn eine lokale Appliance ausfällt und repariert werden muss, kann der Internetzugriff ausfallen und die Sicherheitslage gefährdet sein, falls ein Fail-Open über das Web zugelassen wurde. Bei einem Fehler in einem unserer Rechenzentren leitet unser Cloud-Dienst den gesamten Web-Datenverkehr zum schnellsten, nächstgelegenen Rechenzentrum um, sodass der Betrieb weiterhin gewährleistet ist.

Darüber hinaus kann unsere Cloud-Dienst-Architektur als „Peer“ mit dem Internet-Backbone an den größten Internetknoten (IXPs) der Welt kommunizieren. So entfallen Routing-Hops vermittelnder Internet-dienstanbieter (ISPs), die die Latenz der Verbindung erhöhen würden. Durch die geringe Anzahl der Hops bei der Verbindung zu beliebten Inhaltsanbietern wie Microsoft Office 365 und Google erhalten die Benutzer mit unserem Cloud-Dienst schnellere Verbindungen als über das offene Internet.

Wichtige Vorteile (Fortsetzung)

- Bewährte Architektur: McAfee Web Gateway Cloud Service ist als Mehrmandantenversion von McAfee Web Gateway konzipiert, der lokalen Appliance, der Unternehmen auf der ganzen Welt vertrauen

McAfee Web Gateway Cloud Service ist global. Web-Inhalt kann in der jeweiligen Landessprache bereitgestellt werden. So erhält ein Benutzer beispielsweise an jedem Zugriffsort lokale Google-Suchergebnisse. Einen Überblick über die aktuellen Standorte und den Status der Rechenzentren, in denen Web-Datenverkehr verarbeitet wird, finden Sie unter https://trust.mcafee.com.

Abwehr raffinierter Bedrohungen

Sicherheitsteams sind bei extrem raffinierter Malware und gezielten Angriffen, die herkömmliche Abwehrmaßnahmen umgehen, häufig im Nachteil. Folgen sind eine starke Bindung von Ressourcen und ständige „Feuerwehreinsätze“, um bei der Behebung der Endgeräteprobleme Schritt zu halten. Im Gegensatz zur herkömmlichen URL-Filterung und zu signaturbasierten Ansätzen bei der Abwehr von Web-Bedrohungen schützt McAfee Web Gateway Cloud Service Endgeräte mittels Inline-Emulation von Dateien, JavaScript und HTML vor Zero-Day- und dateiloser Malware. Zero-Day-Malware wird zum Beispiel bereits bekämpft, bevor sie den Benutzer erreicht. Zudem verbessert sich die Blockierungsrate um etwa 20 Prozent im Vergleich zur URL-Filterung und zu signaturbasierten Lösungen. Das Sicherheitskontrollzentrum profitiert von geringeren Kosten und flexibleren Ressourcen, weil die Gesamtzahl der Malware-Vorfälle sinkt. Alle noch verbleibenden verdächtigen Dateien können an McAfee Cloud Threat Detection gesendet werden. Diese Cloud-basierte Lösung zur erweiterten Bedrohungsanalyse ist als kostenloser Dienst verfügbar, der nativ bereits in McAfee Web Gateway Cloud Service enthalten ist.

Web-Bedrohungen werden oft im verschlüsselten Datenverkehr transportiert, um sich vor Abwehrmechanismen der Web-Sicherheitsmaßnahmen zu verstecken. Nahezu alle Cloud-Anwendungen, wie Cloud-Speicher oder soziale Medien, nutzen standardmäßig verschlüsselten Datenverkehr. McAfee Web Gateway Cloud Service kann HTTPS-verschlüsselten Datenverkehr vollständig entschlüsseln und inspizieren, um Malware abzuwehren und Cloud-Anwendungen in verschlüsselten Kanälen sichtbar zu machen.

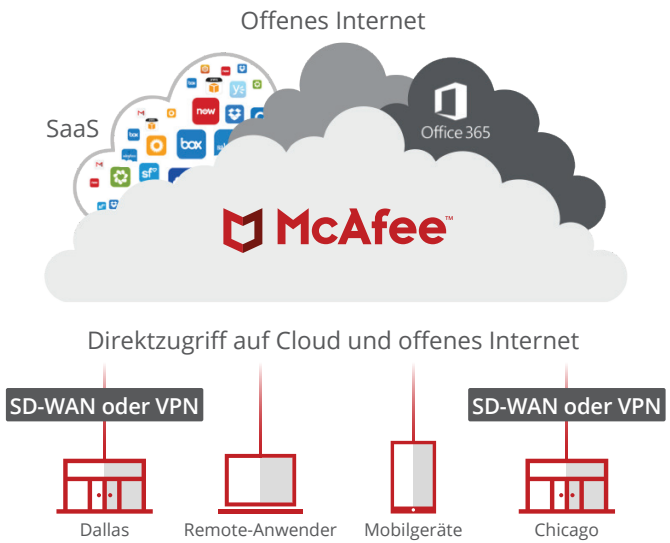

Abbildung 1. Cloud-native Architektur für Web- und Cloud-Sicherheit

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. Durch die Zentralisierung von McAfee Web Gateway Cloud Service und McAfee MVISION Cloud (CASB) können Sie über eine einzige Konsole den Zugriff auf alle Cloud-Dienste steuern und diese Dienste vor Bedrohungen schützen.

Die kombinierten Richtlinien ermöglichen bisher unerreichte Cloud-Kontrolle, wobei MVISION Cloud über API und Reverse-Proxy die notwendige Transparenz und Kontrolle für genehmigte Cloud-Dienste bietet. Parallel dazu überwacht und blockiert McAfee Web Gateway Cloud Service per Forward-Proxy nicht genehmigte Cloud-Dienste sowie den Web-Datenverkehr. Besonders riskante Cloud-Dienste werden blockiert, um Zugriffe von Endbenutzern auf diese Dienste zu verhindern und vor versehentlichen Datenverlusten und Malware-Infektionen zu schützen.

Wo finde ich McAfee Web Gateway Cloud Service?

Unter https://trust.mcafee.com erhalten Sie Live-Updates und einen Überblick über die Standorte unserer Rechenzentren, Verfügbarkeitsstatus und mehr.

Weitere Informationen

Weitere Informationen finden Sie unter www.mcafee.com/de/products/web-gateway-cloud-service.aspx.

McAfee

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