McAfee Web Gateway

Sicherheit. Vernetzte Daten. Leistung.

Unternehmen stehen heute über das Internet viel mehr Möglichkeiten offen als je zuvor. Das Web ermöglicht eine dynamische Arbeitsweise in Echtzeit. Es birgt jedoch auch viele Gefahren, und die Angriffsmethoden werden immer raffinierter. McAfee® Web Gateway ist für jedes Unternehmen eine unverzichtbare Schutzmaßnahme gegen neue Malware-Bedrohungen. Die Lösung nutzt einen fortschrittlichen Sicherheitsansatz, der leistungsstarke, lokale Absichtsanalysen mit Cloud-basiertem Schutz durch McAfee Labs kombiniert. Dadurch können Unternehmen ihren Mitarbeitern unbesorgt sicheren Zugang zum Internet gewähren und gleichzeitig das Risiko erheblich senken.

McAfee Web Gateway

- Zertifizierung nach Common Criteria EAL2+ und FIPS 140-2 Level 2
- Verfügbar in verschiedenen Hardware-Modellen und als virtuelle Maschine, die VMware und Microsoft Hyper-V unterstützt
- In ergänzende Intel® Security-Lösungen wie McAfee Advanced Threat Defense und McAfee Threat Intelligence Exchange integriert
- Als Nr. 1 bewertete Malware-Schutzlösung in einem sicheren Web-Gateway (AV-TEST)

Mit zunehmender Nutzung und Weiterentwicklung des Internets steigt auch der Bedarf nach fortschrittlicher Web-Sicherheit. Selbst scheinbar „sichere“ Webseiten können angegriffen und zur Malware-Verbreitung missbraucht werden.

In der heutigen Zeit reicht es nicht aus, bekannte Viren zu blockieren oder den Zugriff auf als gefährlich eingestufte Webseiten zu beschränken. Reaktive Techniken, wie zum Beispiel signaturbasierter Virenschutz und auf Kategorien beschränkte URL-Filterung, sind zwar unverzichtbare Schutzmaßnahmen, können aber den Zugang zu Cloud-Anwendungen nicht absichern und sind nicht darauf ausgelegt, aktuelle Bedrohungen abzuwehren.

Da sich diese Lösungen auf bekannte Inhalte und gefährliche Objekte sowie ausführbare Dateien konzentrieren, können sie heutige Angriffe, bei denen gefährlicher Code in scheinbar harmlosem HTTP- oder HTTPS-Verkehr versteckt wird, weder verhindern noch Schutz vor unbekannten oder neuen Bedrohungen bieten. Es gilt, sicheren, detailliert geregelten Zugang zu Cloud-Anwendungen zu gewähren und gleichzeitig bekannte sowie unbekannte Bedrohungen präventiv abzuwehren.

Umfassender Schutz ein- und ausgehender Daten

McAfee Web Gateway bietet dank einer Hochleistungs-Appliance-Software-Architektur umfassende Sicherheit für alle Bereiche des Web-Datenverkehrs. Sobald ein Anwender eine Web-Anfrage startet, wendet McAfee Web Gateway zunächst die im Unternehmen geltenden Richtlinien zur Internetnutzung an. Der gesamte zulässige Datenverkehr wird dann mithilfe lokaler und globaler Analyseverfahren auf Art und Absicht des Inhalts sowie des aktiven Codes geprüft, der von den angefragten Webseiten ins Netzwerk übertragen wird. Dadurch wird ein unmittelbarer Schutz vor Malware und anderen versteckten Bedrohungen ermöglicht. Im Gegensatz zu grundlegenden Paketanalyseverfahren kann McAfee Web Gateway auch SSL-Datenverkehr untersuchen und so einen tiefgreifenden Schutz vor schädlichem Code gewährleisten oder Anwendungen kontrollieren, die durch Verschlüsselung verborgen wurden.

intel Security

Der Schutz für eingehende Daten senkt auch das Risiko für Unternehmen mit eigenen Webseiten, die Dateneingaben oder Dokumenten-Uploads aus externen Quellen akzeptieren. Im umgekehrten Proxy-Modus kann McAfee Web Gateway sämtliche Inhalte bereits vor dem Upload scannen und auf diese Weise sowohl den Server als auch den Inhalt absichern.

Zum Schutz ausgehender Daten scannt McAfee Web Protection mithilfe der branchenweit führenden Intel® Security Data Loss Protection-Technologie sämtliche wichtigen Internetprotokolle wie HTTP, HTTPS und FTP auf benutzergenerierte Inhalte. Die Lösung schützt auch vor der Exfiltrierung vertraulicher, sensibler oder regulierter Informationen aus dem Unternehmen durch soziale Netzwerke, Blogs, Wikis oder Online-Tools zur Produktivitätssteigerung wie webbasierte E-Mails, Organizer und Kalender. McAfee Web Gateway schützt auch vor der nicht autorisierten Weitergabe von Daten über von Bots infizierte Geräte, die versuchen, „nach Hause zu telefonieren“ oder sensible Daten zu übertragen.

Branchenweit bester Schutz

Die bestbewertete Malware-Sicherheitslösung[1] verwendet mit der McAfee Gateway Anti-Malware Engine eine patentierte Technik zur signaturlosen Absichtsanalyse. Die präventive Absichtsanalyse filtert in Echtzeit bislang unbekannte oder Zero-Day-Schaddaten aus dem Web-Datenverkehr heraus. Durch Scannen des aktiven Inhalts einer Webseite, Emulieren sowie Erfassen seines Verhaltens und Vorhersagen seiner Absicht schützt McAfee Web Gateway vor der Übertragung von Zero-Day-Malware auf Endgeräte. Dadurch kann die Lösung die Kosten für Systembereinigung und Wiederherstellung erheblich senken.

Diese Analysen werden mit Intel Security-Virenschutz sowie weltweiten McAfee Labs-Reputationsanalysen kombiniert, um bekannte Malware und gefährliche Webseiten schnell zu blockieren. Durch die Nutzung verschiedener, aber sich gegenseitig ergänzender Technologien kann McAfee Web Gateway mehr Schutz sowie optimale Sicherheit auf einer einzigen Plattform bieten und damit genau den tiefgreifenden Schutz gewährleisten, den viele Unternehmen benötigen.

- **McAfee-Virenschutz mit dem Echtzeit-Datei-Reputationsdienst McAfee Global Threat Intelligence (McAfee GTI):** Der Cloud-basierte Datei-Reputationsdienst McAfee GTI schließt die Lücke zwischen Virenerkennung und Systemaktualisierung bzw. -schutz.
- **Reputations-Analyse und Kategorisierung von Webseiten mit McAfee GTI:** McAfee Web Gateway bietet mit einer leistungsstarken Kombination aus reputations- und kategoriebasierter Filterung Filter- und Schutzfunktionen für den Zugriff auf das Internet. McAfee GTI erstellt ein Profil aller Internet-Präsenzen (Webseiten, E-Mail- und IP-Adressen) auf der Grundlage von Hunderten verschiedenen Attributen, die durch die umfangreichen weltweiten Datenerfassungskapazitäten von McAfee Labs erfasst werden. Anschließend ordnet die Lösung Reputations-Bewertungen zu, die auf dem ermittelten Sicherheitsrisiko beruhen und es Administratoren ermöglichen, detaillierte Regeln für zulässige oder unzulässige Aktivitäten zu erstellen.
- **Geografischer Standort:** McAfee Web Gateway berücksichtigt den geografischen Standort und ermöglicht so eine geografische Übersicht sowie Richtlinien für das Ursprungsland des Datenverkehrs sowie des Benutzers.

Sowohl bei der Web-Kategorisierung als auch bei der Reputations-Analyse können Unternehmen zwischen einer Lösung vor Ort, in der Cloud oder einer Kombination aus beidem wählen. Cloud-basierte Suchen schließen die Lücke zwischen der Entdeckung/Änderung und System-Updates und bieten mit Daten von hunderten Millionen eindeutigen Malware-Varianten eine breite Abdeckung.

Integration von Advanced Threat Defense
McAfee Web Gateway integriert sich in McAfee Advanced Threat Defense, die fortschrittliche Malware-Erkennungstechnologie von Intel Security, die anpassbare Sandbox-Analysen mit gründlicher statischer Code-Analyse kombiniert. McAfee Advanced Threat Defense bietet zusammen mit den Inline-Scan-Funktionen der Gateway Anti-Malware Engine von McAfee Web Gateway den stärksten Schutz vor Bedrohungen, die über das Internet übertragen werden.

Austausch von Bedrohungsdaten
Heute agieren die Sicherheitsarchitekturen vieler Unternehmen isoliert – ein Austausch von Bedrohungsdaten untereinander ist nicht vorgesehen, obwohl wichtige Sicherheitsdaten auf Endgeräten, dem Netzwerk, Sicherheits-informations- und Ereignis-Management-Lösungen, Gateways usw. anfallen. Wenn diese Bedrohungsdaten geteilt werden, können sie den Schutz vor Bedrohungen stärken, die Erkennung von Kompromittierungen verbessern und die effiziente Behebung kompromittierter Systeme ermöglichen. Intel Security-Lösungen wie McAfee Web Gateway tauschen jedoch über McAfee Threat Intelligence Exchange Bedrohungsdaten untereinander aus, um diese Lücken zu schließen. McAfee Web Gateway bietet dabei enormen Mehrwert, weil die Lösung neue Datei-Reputationen für von der Gateway Anti-Malware Engine erkannte Zero-Day-Malware erstellt und weitergibt. Dadurch können beispielsweise Endgeräte geschützt werden, noch bevor eine neue DAT-Datei veröffentlicht wird. Außerdem werden dank der erweiterten Bedrohungsdaten von McAfee Threat Intelligence Exchange weitere Bedrohungen von McAfee Web Gateway gestoppt.

Schutz verschlüsselter Daten
Mit dem SSL-Datenverkehr (HTTPS) haben raffinierte Cyber-Kriminelle eine Hintertür zur Umgehung der Sicherheitssperren von Unternehmen aufgestoßen. Ironischerweise muss ein Protokoll, das für höhere Sicherheit konzipiert wurde, ebenfalls auf Risiken untersucht werden. McAfee Web Gateway ist das erste Sicherheitsprodukt, das Malware-Erkennung, SSL-Prüfung und Zertifikatsvalidierung vollständig integriert. Verschlüsselte Daten müssen nicht an ein separates Gerät geleitet werden, um dort eine SSL-Prüfung durchzuführen. McAfee Web Gateway scannt den gesamten SSL-Datenverkehr unmittelbar und gewährleistet vollständige Sicherheit, Integrität sowie die Vertraulichkeit verschlüsselter Transaktionen.

Schutz vor Datenverlust
Durch das protokollübergreifende Scannen ausgehender Inhalte (einschließlich SSL) schützt McAfee Web Gateway Unternehmen vor Bedrohungen durch ausgehende Daten, z. B. dem Verlust vertraulicher Informationen. Daher ist McAfee Web Gateway ein leistungsstarkes Tool zum Schutz von geistigem Eigentum, zur Gewährleistung und Dokumentation gesetzlicher Compliance sowie zur Bereitstellung forensischer Daten im Falle von Kompromittierungen. McAfee Web Gateway greift auf McAfee Data Loss Prevention (DLP) zu und nutzt die integrierten DLP-Wörterbücher. Zudem können Sie mithilfe von Kennwortabgleich und/oder regulären Ausdrücken benutzerdefinierte Wörterbücher erstellen.

Bei Unternehmen, die Cloud-basierten Speicher nutzen, schützt die integrierte Dateiverschlüsselung auf Dateiaustauschseiten hochgeladene Daten vor unbefugtem Zugriff. Die Benutzer können die Daten nur dann abrufen und anzeigen, wenn sie über McAfee Web Gateway darauf zugreifen.

Schutz für Benutzer außerhalb des Netzwerks
Angesichts der zunehmenden Verteilung und Mobilität von Angestellten wird die Notwendigkeit von Web-Filterung und Schutz für den nahtlosen Übergang vom Büro zum mobilen Arbeitsplatz immer wichtiger. Mit dem manipulationssicheren Client-Agenten McAfee Client Proxy können sich Benutzer mit Fernzugriff nahtlos authentifizieren und werden zu einem lokalen Web-Gateway in einer DMZ oder an den McAfee Web Gateway Cloud Service weitergeleitet. Dadurch können Internetzugriffsrichtlinien durchgesetzt und die Remote- bzw. Mobil-Anwender vollständigen Sicherheits-Scans unterzogen werden. Das gilt selbst dann, wenn deren Internetzugriff über

ein öffentliches Portal erfolgt, wie es häufig bei Schnellrestaurants, Hotels oder anderen WLAN-Hotspots der Fall ist.

Mit McAfee Web Gateway können Unternehmen ihre Sicherheitsrichtlinien zudem auf den Mobilbereich ausweiten und auf Mobilgeräten durchsetzen, indem der Web-Datenverkehr über den McAfee Web Gateway geleitet wird. McAfee Web Gateway gewährleistet mithilfe standardmäßiger Geräte-Management- und Sicherheitsfunktionen, dass Mobilgeräte mit fortschrittlichem Malware-Schutz und Internetfilterrichtlinien des Unternehmens abgesichert werden. Die Lösung schützt darüber hinaus auch beim Zugriff von Mobilgeräten auf Inhalte, die üblicherweise auf internen Unternehmens-Servern wie Intranets, Wikis, Microsoft SharePoint-Servern und anderen webbasierten Lösungen gespeichert werden. In der Regel werden solche Informationen aufgrund von Sicherheitsbedenken generell gegen den Zugriff von bestimmten Mobilgeräten aus gesperrt. Wenn jedoch McAfee Web Gateway als umgekehrter Proxy eingesetzt wird, ist ein kontrollierter und sicherer Zugriff auf diese internen Ressourcen möglich.

Maximale Flexibilität

McAfee Web Gateway bietet ein leistungsfähiges, regelbasiertes Modul für flexible Richtlinien und Kontrollen. Zur Optimierung der Richtlinienerstellung bietet McAfee Web Gateway eine umfassende Bibliothek mit vordefinierten Regeln für häufig genutzte Maßnahmen. Unternehmen können zwischen verschiedenen Regeln wählen, diese einfach modifizieren und eigene Regeln über eine Online-Community weitergeben. Die Verwaltung wird durch eine einmalige Kombination aus kontextbasierten Regelkriterien und gemeinsamen Listen verbessert, die unbegrenzte Möglichkeiten zur Lösung von Problemen und Optimierung der Web-Sicherheit bietet. Die interaktive Regelverfolgung vereinfacht das Regel-Debugging erheblich.

McAfee Web Gateway dehnt die Kontrolle auch auf Cloud-Anwendungen aus und ermöglicht so eine detaillierte, Proxy-basierte Kontrolle der Nutzung von Web-Anwendungen. Unternehmen können mehr als 1.600 Kontrollen für Cloud-Anwendungen nutzen und spezifische Funktionen nach Bedarf aktivieren oder deaktivieren sowie kontrollieren, von wem und wie Web-Anwendungen genutzt werden. Möchten Sie den Zugriff auf Dropbox ermöglichen, aber Uploads sperren? Kein Problem.

Die Flexibilität und Kontrollmöglichkeiten umfassen auch die Anwenderauthentifizierung und Zugriffssteuerung. So unterstützt McAfee Web Gateway zahlreiche Authentifizierungsverfahren wie NTLM, RADIUS, AD/LDAP, eDirectory, Kerberos oder die Authentifizierung per Cookie oder lokaler Benutzerdatenbank. Mithilfe des Authentifizierungsmoduls von McAfee Web Gateway können Administratoren flexible Regeln implementieren, darunter auch die Nutzung mehrerer Authentifizierungsverfahren. Beispielsweise kann McAfee Web Gateway versuchen, einen Benutzer mit einem transparenten Verfahren zu authentifizieren und ihn dann je nach Ergebnis zur Eingabe von Anmeldedaten auffordern, ein weiteres Authentifizierungsverfahren einsetzen, eine restriktive Richtlinie anwenden oder einfach den Zugriff verweigern.

McAfee Web Gateway Identity, ein optionales Add-On, bietet SSO-Connector-Module (Single Sign-On) für hunderte beliebte Cloud-basierte Anwendungen. Im SSO Launch Pad von McAfee Web Gateway Identity können Benutzer mit einem einzigen Mausklick auf autorisierte Cloud-Anwendungen zugreifen. Dadurch können Sie die Sicherheit verbessern und die Anzahl kennwortbezogener Helpdesk-Anrufe reduzieren. Dank der Unterstützung für HTTP POST sowie SAML-Connector-Module (Security Assertion Markup Language) wird ein großes Spektrum an Anwendungen abgedeckt. Mithilfe von Bereitstellungs-Connector-Modulen können Systemadministratoren Benutzerkonten für ausgewählte SaaS-Anwendungen (Software-as-a-Service) erstellen und entfernen.

McAfee Web Gateway dehnt die Zugriffskontrolle durch integrierte Streaming-Proxy-Unterstützung auch auf Streaming-Inhalte aus und reduziert so die Netzwerkauslastung sowie Latenzen. Weitere Bandbreitenkontrollen können eingerichtet werden, um minimale und maximale Werte durchzusetzen. Zudem können bestimmten Datenverkehrtypen Prioritäten zugeordnet werden, um die optimale Nutzung der verfügbaren Bandbreite zu gewährleisten.

Flexible Infrastruktur und Leistung

McAfee Web Gateway ist ein unternehmensgerechter Hochleistungs-Proxy in einer skalierbaren Appliance-Familie mit integrierter Hochverfügbarkeit, Unterstützung für virtuelle Maschinen sowie Hybrid-Bereitstellungen mit **McAfee Web Gateway Cloud Service**. McAfee Web Gateway bietet Bereitstellungsflexibilität sowie -leistung und ist so weit skalierbar, dass sogar Hunderttausende Benutzer in einer Umgebung problemlos unterstützt werden können.

Sie haben auch die Möglichkeit, unterschiedliche Bereitstellungsmethoden zu wählen. Beispielsweise können Sie den gesamten Web-Datenverkehr für Benutzer im Netzwerk zur lokalen Appliance und für Benutzer außerhalb des Netzwerks an den Cloud-Dienst leiten. Dadurch sparen Sie die Kosten für das Backhauling von Datenverkehr über MPLS- oder VPN-Verbindungen. Automatisierte Richtliniensynchronisation und Berichterstellungsfunktionen für hybride Vor-Ort- und Cloud-Implementierungen vereinfachen die Optimierung der Verwaltung, gewährleisten konsistente Richtliniendurchsetzung und vereinfachen Berichterstellung, Nachverfolgung sowie Untersuchungen.

McAfee Web Gateway lässt sich auf verschiedenste Art und Weise implementieren, etwa als expliziter Proxy, als transparente Bridge oder als Router. So ist sichergestellt, dass Ihre jeweilige Netzwerkarchitektur unterstützt wird.

Durch die Unterstützung zahlreicher Integrationsstandards kann McAfee Web Gateway auch in sehr individuellen Umgebungen eingesetzt werden. McAfee Web Gateway kommuniziert über das Web Cache Communication Protocol (WCCP), das Internet Content Adaptation Protocol (ICAP/ICAPS), das WebSocket-Protokoll sowie das Socket Secure-Protokoll (SOCKS) effizient mit anderen Netzwerkgeräten und Sicherheits-Appliances.

Darüber hinaus unterstützt McAfee Web Gateway auch IPv6 und erleichtert Großunternehmen sowie staatlichen Einrichtungen die Einhaltung entsprechender Vorschriften. McAfee Web Gateway verbindet interne IPv4- sowie externe IPv6-Netzwerke und setzt alle verfügbaren Sicherheits- sowie Infrastrukturfunktionen zur Überprüfung des Datenverkehrs ein.

Einheitliche zukunftsfähige Plattform

McAfee Web Gateway kombiniert und integriert zahlreiche Schutzfunktionen, für die normalerweise mehrere Einzelprodukte erforderlich wären. URL-Filterung, Virenschutz, Zero-Day-Malware-Schutz, SSL-Scans, Schutz vor Datenkompromittierung und zentrale Verwaltung sind alle in einer einzigen Appliance-Software-Architektur vereint. Die Verwaltung von Bereitstellungen erfolgt einheitlich für alle Formfaktoren, sodass eine Richtlinie mithilfe einer einzigen Verwaltungskonsole auf lokalen Appliances, Appliance-Clustern, virtuellen Appliances und dem Cloud-Dienst bereitgestellt werden kann.

Sicherheitsrisiko-Management und Reporting

McAfee ePolicy Orchestrator® (McAfee ePO™), die beliebte und anerkannte Sicherheits-Management-Plattform, dient McAfee Web Gateway als zentrale Quelle für alle Sicherheitsberichte.

Über die Erweiterung McAfee Content Security Reporter unterstützt McAfee ePO detaillierte Web-Sicherheitsberichte. McAfee Content Security Reporter stellt Ihnen Informationen und forensische Tools bereit, mit denen Sie die Web-Nutzung in Ihrem Unternehmen nachvollziehen, Instanzen unbekannter oder nicht autorisierter „Schatten-IT"-Anwendungen ermitteln, gesetzliche Vorschriften einhalten, Trends erkennen, Probleme identifizieren und Ihre Filtereinstellungen so anpassen können, dass Ihre Web-Sicherheitsrichtlinien auch durchgesetzt werden. Mit McAfee Content Security Reporter erhalten Sie einen externen, eigenständigen Berichterstellungs-Server, der den McAfee ePO-Server von der ressourcenintensiven Datenverarbeitung und -speicherung entlastet. Dadurch kann die Lösung die Berichterstellung selbst für die weltweit größten Unternehmen übernehmen.

Lizenzierung

Wenn Sie die größtmögliche Flexibilität bei der Bereitstellung erhalten und die Zukunftssicherheit Ihrer Investition sicherstellen möchten, bietet Ihnen Intel Security sämtliche Funktionen von McAfee Web Gateway und McAfee Web Gateway Cloud Service in einer kompletten Suite: **McAfee Web Protection**. Sie haben die freie Wahl zwischen der Bereitstellung vor Ort oder in der Cloud – oder Sie nutzen eine kombinierte Strategie für mehr Flexibilität und höhere Verfügbarkeit. Auf den preisgekrönten Malware-Schutz und die umfassende Web-Filterung von Intel Security können Sie sich in jedem Fall verlassen.

Die McAfee Web Gateway-Hardware wird separat angeboten.

1. In Tests von AV-TEST erkannte McAfee Web Gateway 94,5 % aller Zero-Day-Malware-Exemplare, 99,8 % aller böswilligen Windows 32-PE-Dateien (Portable Executable) sowie 98,63 % aller nicht-PE-Dateien. „McAfee Web Gateway Security Appliance Test" (Test der Sicherheits-Appliance McAfee Web Gateway), AV-TEST GmbH.

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