McAfee Email Gateway

Schutz von E-Mails im Unternehmen

Hauptvorteile

Vollständiger Schutz ein- und ausgehender Daten

- Umfassender Schutz vor allen Bedrohungen in eingehenden E-Mails
- Integrierte E-Mail-Verschlüsselung
- Integrierte Compliance-Vorlagen und Schutz vor Datenkompromittierung für sensible Informationen

Fortschrittliche Sicherheit, Verwaltung und Skalierbarkeit

- Verfügbar als virtuelle Appliance, Hardware-Appliance, Blade-Server oder als integrierte Hybrid-Lösung mit McAfee SaaS Email Protection
- Zentrale Verwaltung, Nachrichtensuche, Berichterstellung und Quarantäne
- Clustering und integrierte Lastverteilung für bessere Skalierbarkeit, um selbst die anspruchsvollsten Anforderungen von Vor-Ort-Umgebungen zu erfüllen

Profitieren Sie von der Nutzung des Security Connected-Ansatzes durch die Lösungen McAfee® ePolicy Orchestrator® (McAfee ePO™), McAfee Global Threat Intelligence (McAfee GTI), McAfee Advanced Threat Defense sowie den Hybrid-Sicherheitsansatz für E-Mails.

E-Mails sind unverzichtbar und einer der wichtigsten Dienste in jeder Unternehmensumgebung. Ihre Fähigkeit, verschiedenste Informationen innerhalb weniger Augenblicke über organisatorische, geographische und politische Grenzen hinweg zu transportieren, machen sie zu einem wesentlichen Hilfsmittel – und zu einer erheblichen Herausforderung für die Sicherheit. McAfee® Email Gateway verbessert Ihre E-Mail-Sicherheit durch die Integration von Schutz vor Bedrohungen in eingehenden E-Mails, die Vermeidung von Datenkompromittierung durch ausgehende E-Mails, Verschlüsselungsfunktionen, fortschrittliche Compliance-Funktionen und die zentrale Verwaltung in einer einzelnen benutzerfreundlichen Appliance.

Sicherheitsprobleme bei E-Mails

Unternehmen sehen sich heute folgenden schwerwiegenden Problemen bei der E-Mail-Sicherheit gegenüber:

- Angriffe über eingehende E-Mails sind immer häufiger das Werk organisierter Krimineller, die nach finanziell ausbeutbaren Informationen suchen. Diese Angriffe setzen auf ausgefeilte Social-Engineering-Techniken und ändern sich in hohem Tempo, um herkömmliche, signaturbasierte Verteidigungsmaßnahmen zu umgehen.
- E-Mail ist auch einer der bedeutendsten Kanäle, über die vertrauliche Daten kompromittiert werden oder verloren gehen – sei es durch gutgesinnte, aber arglose Mitarbeiter oder durch böswillige Insider.
- Da E-Mails für betriebliche Abläufe wichtig sind und zugleich eine verbreitete Schwachstelle darstellen, unterliegen sie zunehmend länder- sowie branchenübergreifenden Vorschriften. Zu den bestehenden Vorgaben zählen der Standards Payment Card Industry Data Security Standard (PCI DSS) für Kreditkartentransaktionen, der Gramm-Leach-Bliley Act (GLBA) im Finanzsektor, der Health Insurance Portability and Accountability Act (HIPAA) im Gesundheitssektor sowie der Sarbanes-Oxley-Act (SOX) für alle in den USA börsennotierten Unternehmen.
- Schätzungen gehen davon aus, dass es sich bei 75 Prozent des weltweiten E-Mail-Aufkommens um Spam handelt, wobei es zwischen den einzelnen Ländern erhebliche Unterschiede gibt. Das Spearphishing wird immer gezielter eingesetzt, ist stärker finanziell ausgerichtet und geht immer effektiver vor.
- McAfee Labs erfasste im 4. Quartal 2013 etwa 2.250 Phishing-URLs am Tag, wobei die Zahlen im Verlauf des Jahres relativ konstant blieben.

intel Security

Auszeichnungen für 2013

- Im Gartner Magic Quadrant als führender Anbieter für sichere E-Mail-Gateways eingestuft
- Laut Forrester Wave führende Position beim Schutz von E-Mail-Inhalten
- Fünf Sterne und Auszeichnung als „Best Buy" (Bestes Produkt) vom *SC Magazine* für „Besten Schutz von E-Mail-Inhalten"
- Laut *SC Magazine* Brancheninnovator im Bereich Datensicherheit

Besser als fragmentierte und ungeeignete Schutzmaßnahmen

Die E-Mail-Sicherheitsmaßnahmen im Unternehmen haben sich erheblich weiterentwickelt. Dabei ist jedoch auffällig, dass die meisten bestehenden E-Mail-Schutzlösungen ausschließlich eingehende E-Mails erfassen und keinen Schutz vor Datenverlusten durch ausgehende E-Mails bieten. Das bedeutet, dass meist eine Vielzahl von Einzelprodukten zum Schutz vor Malware, Spam, Phishing, Viren und Datenkompromittierung sowie für Verschlüsselung eingesetzt wird, die von verschiedenen Anbietern stammen, getrennt voneinander implementiert und mehrfach aufgerüstet werden. Viele erfüllen nicht die derzeit empfohlenen Leistungsstandards.

So erreichen führende Spam-Schutzlösungen eine Erkennungsgenauigkeit von 99 Prozent oder mehr, während viele E-Mail-Schutzvorkehrungen lediglich 95 Prozent oder noch weniger schaffen. Ein Unterschied von 4 Prozent mag unbedeutend klingen, er wirkt sich jedoch in Form einer um 400 Prozent höheren Anzahl durchgelassener Spam-Mails und damit auch potenzieller Systeminfektionen aus. In Zeiten, in denen das Spam-Aufkommen in Milliarden E-Mails gemessen wird, kann sich ein Anstieg um 4 Prozent erheblich auf die Geschäftsabläufe auswirken. So können durch 4 Prozent mehr E-Mails die Infrastruktur überlastet oder die verfügbare Bandbreite stark reduziert werden. Selbst wenn nur ein Bruchteil der unerwünschten E-Mails die Schutzvorkehrungen überwindet, werden Benutzer durch das Sichten und Löschen von Spam-E-Mails von ihrer eigentlichen Arbeit abgelenkt. Gleichzeitig steigt das Risiko einer Malware-Infektion und damit auch die Gefahr von Kostensteigerungen, Produktivitäts- sowie potenziellen Datenverlusten.

Dies führt zwangsläufig dazu, dass die meisten IT-Organisationen zu viel Zeit und Geld für die Pflege unzusammenhängender Einzelschutzmaßnahmen, den Schutz sensibler Informationen vor Kompromittierung, den Nachweis der Richtlinien-Compliance und die Beseitigung der Folgen von unzureichender E-Mail-Sicherheit aufwenden müssen. Somit sprechen überzeugende geschäftliche Argumente für eine umfassende E-Mail-Sicherheitslösung mit gebündelten Schutzvorkehrungen für ein- sowie ausgehenden E-Mail-Verkehr, die die Verwaltung vereinfacht und die Richtlinieneinhaltung optimiert. Der Name dieser Lösung: McAfee Email Gateway.

Umfassender E-Mail-Schutz

Marktführende Sicherheit

McAfee Email Gateway vereint fortschrittlichen Schutz vor eingehenden Bedrohungen mit Schutzmaßnahmen gegen Datenverluste durch ausgehende E-Mails sowie fortschrittliche Compliance- und E-Mail-Verschlüsselungsfunktionen, hoher Leistung, Berichten und einheitlicher Verwaltung – auf einer einzigen, gesicherten Plattform zu einem Einheitspreis.

- Durch die Kombination von Daten aus dem lokalen Netz und Reputations-Daten, die über McAfee GTI bereitgestellt werden, bietet die Lösung den lückenlosesten erhältlichen Schutz vor eingehenden Bedrohungen, Spam und Malware.
- Dank der Link-Scans zum Klick-Zeitpunkt in Kombination mit Verhaltensemulationsfunktionen der McAfee Gateway Anti-Malware Engine werden Angriffe abgewehrt, die auf böswillige URLs setzen.
- Die Integration in McAfee Advanced Threat Defense ermöglicht dank der innovativen Kombination statischer und dynamischer (Sandbox-)Analysen die Erkennung höchst raffinierter und verschleierter Malware.
- Seine ausgefeilten Inhalts-Scan-Technologien, die zahlreichen Verschlüsselungsverfahren sowie ein präzise festlegbarer, richtlinienbasierter Umgang mit Nachrichten schützen vor Datenkompromittierung und vereinfachen die Richtlinieneinhaltung.
- Dank der vollständigen Integration in die Software McAfee ePO kann die Lösung innerhalb eines oder mehrerer Cluster vollständig verwaltet werden. Durch die unternehmensgerechten Protokollierungs- und Berichterstellungsfunktionen, die die Verwaltung und den Compliance-Nachweis vereinfachen, werden zudem erheblich Kosten eingespart.

Umfassender Schutz vor eingehenden Bedrohungen
McAfee Email Gateway erkennt sowie blockiert eingehende Spam-E-Mails mit einer Genauigkeit von mehr als 99 Prozent und bietet integrierten Schutz vor Viren, Malware, Phishing-, Directory-Harvest-, Denial-of-Service- sowie Bounce-back-Angriffen. Die Lösung wehrt Zero-Hour-Bedrohungen, gezielte sowie komplexe Angriffe ab und verringert durch eine leistungsstarke Kombination von dynamischer Spam-Klassifizierung und Reaktionen auf Bedrohungen erheblich die Folgen von Spam-Lawinen. McAfee Email Gateway bleibt dank der Reputationsdaten von McAfee GTI für Absender, E-Mails und URLs stets auf dem neuesten Stand.

McAfee Email Gateway enthält ein zweites Virenschutzmodul, das unseren Kunden mehrschichten Schutz vor Malware bietet und sie bei der Erfüllung von Compliance-Anforderungen unterstützt.

Dadurch, dass Links zum Zeitpunkt des Klickens geprüft werden, können auch neue Angriffe abgewehrt werden.
Die in McAfee Email Gateway enthaltene Funktion McAfee ClickProtect bietet Schutz vor Bedrohungen durch eingebettete URLs in E-Mail-Nachrichten. Diese Funktion analysiert Veränderungen beim Ziel der URL zwischen dem Zeitpunkt des E-Mail-Scans und dem Zeitpunkt, zu dem der Benutzer auf den Link klickt. Diese Analyse wird auch auf unverdächtig erscheinende URLs angewendet. Bei der erneuten Prüfung wird die URL-Reputation ermittelt und eine Ausführung emuliert. Dabei kommt die branchenweit führende Malware-Schutz-Gateway-Technologie zum Einsatz, die auch in McAfee Web Protection enthalten ist. Administratoren können Richtlinien für den Scan- sowie den Klick-Zeitpunkt konfigurieren und die URL-Emulation aktivieren, um die Benutzer vor gefährlichen URLs zu schützen. Safe Preview bietet eine geschützte Ansicht der aufzurufenden Seiten, wobei von Benutzern erfasste Informationen zusätzlichen Schutz bieten. Damit der Web-Zugriff über E-Mails vollständig gesperrt werden kann, können URLs erkannt und entfernt oder durch einen Hinweis ersetzt werden.

McAfee Advanced Threat Defense erkennt hochentwickelte und verborgene Malware.
McAfee Advanced Threat Defense erkennt aktuelle Stealth- und Zero-Day-Malware mithilfe eines innovativen, mehrstufigen Ansatzes. Dabei werden gründliche statische und dynamische (Sandbox-)Analysen kombiniert, um das tatsächliche Verhalten der Malware zu ermitteln. Durch die enge Integration zwischen McAfee Email Gateway und McAfee Advanced Threat Defense können diese Analysen auf verdächtige E-Mail-Anhänge angewendet werden, damit gefährliche Dateien blockiert werden können, bevor sie den Posteingang erreichen.

Während Methoden mit geringerer Analyselast wie Signaturen und Echtzeitemulation Leistungsvorteile bieten, können mithilfe der vollständigen statischen Code-Analyse sowie der Sandbox detaillierte Malware-Klassifizierungsinformationen ermittelt werden. Diese Techniken erweitern auch den Schutz zur Erfassung stark getarnter sowie schwer aufzuspürender Bedrohungen und erlauben die Identifizierung von ähnlicher Malware, die den gleichen Code verwendet. Verzögerte oder verborgene Ausführungspfade, die in einer dynamischen Umgebung häufig nicht ausgeführt werden, können durch das Entpacken und die vollstatische Analyse ermittelt werden.

Gemeinsam ermöglichen die statische Code-Überprüfung und die dynamische Analyse eine vollständige Überprüfung sowie die Erfassung detaillierter Informationen wie Verhalten, Gefährlichkeit der Malware, Einordnung in die Malware-Familie, Ausführungspfade sowie Anteil des Codes, der bei der dynamischen Analyse ausgeführt wird.

Die Graymail-Filterung ermöglicht die weitere Reduzierung unerwünschter E-Mails.
Unerwünschte E-Mails können legitim sein, wenn sie einstmals vom Benutzer angefordert wurden, nun aber nicht mehr erwünscht sind (beispielsweise Branchen-Newsletter und Benachrichtigungen). Graymail wird also nicht unbedingt als Spam angesehen, kann jedoch für die Empfänger eine Belästigung darstellen. Mithilfe von Filtern, die Aktionen wie Blockierung und Quarantäne auslösen, bleiben Ihre Postfächer frei von unerwünschten E-Mails.

Umfassender Schutz ausgehender E-Mails zur Absicherung von Inhalten

Die Lösung beinhaltet E-Mail-Verschlüsselungsfunktionen.

Die standardmäßig integrierte richtlinienbasierte E-Mail-Verschlüsselung nutzt eine Kombination aus B2B- (TLS, S/MIME und OpenPGP) und B2C-Technologien (Push/Pull) und stellt sicher, dass auch Empfänger ohne Verschlüsselungsprogramme verschlüsselte E-Mails empfangen und beantworten können. Die Push/Pull-Technologie umfasst einen individuell anpassbaren Webmail-Client und erlaubt den Abruf sowie die Anzeige verschlüsselter E-Mails auf Mobilgeräten. Durch die Verschlüsselung am Gateway statt auf dem Rechner entfällt die Notwendigkeit für den Benutzer, spezielle Verschlüsselungsregeln festzulegen. Damit wird verhindert, dass der Absender die Verschlüsselung sensibler Daten einfach vergisst.

Sie erhalten Compliance-Funktionen und Schutz vor Datenverlust.

Die Lösung umfasst standardmäßig einen Katalog zuverlässiger integrierter Compliance-Vorlagen, die auch in McAfee Data Loss Prevention zum Einsatz kommen. Dazu zählen Fingerprinting, lexikalische Analyse und Clustering-Techniken, die den Suchbegriffs- und Musterabgleich ergänzen, damit sowohl strukturierte als auch unstrukturierte Daten umfassend erfasst werden können. Der Gateway erkennt zuverlässig regulierte Inhalte (HIPAA, SOX, GLBA), personenbezogene Daten wie Kreditkartennummern, Steuer- und regionalspezifische IDs sowie andere Kunden- und Mitarbeiterdaten. Unstrukturierte Daten und geistiges Eigentum wie Quell-Codes, Patente, Finanzdaten und Geschäftspläne können ebenfalls erkannt und entsprechend gesichert werden. Bei der Erkennung solcher Daten werden abhängig von den geltenden Unternehmensrichtlinien zahlreiche Maßnahmen unterstützt, z. B. die zwangsweise Verschlüsselung (Push, Pull, TLS), Warnungen, Umleitung, Quarantäne, Blockierung sowie weitere kundenspezifische Aktionen.

Umfassendere Möglichkeiten für Administratoren

Mit McAfee Email Gateway können Administratoren optimalen E-Mail-Schutz gewährleisten und ihn mit unternehmensgerechten Berichterstellungsfunktionen, umfassenden exportierbaren Protokollen, konfigurierbaren Echtzeit-Dashboards und Warnungen sowie Detailberichten dokumentieren. Die Lösung verbindet Leistung, Skalierbarkeit sowie Stabilität mit einem flexiblen Bereitstellungsmodell und gewährleistet damit maximale Rendite bei minimalem Aufwand für den Administrator. McAfee Email Gateway kann vollständig über die eigene Verwaltungskonsole oder über die Software McAfee ePO verwaltet werden. Sie bietet zudem folgende weitere Funktionen:

Hochentwickelte Nutzungs- und Richtlinienkontrollen vereinfachen die Verwaltung erheblich.

- Schlanke, intuitive Schnittstelle mit assistentenbasierter Installation und Konfiguration
- Verzeichnis-/LDAP-Integration (Lightweight Directory Access Protocol)
- Zentrale Verwaltung Ihrer E-Mail-Sicherheitsfunktionen mit differenzierter Richtlinienerzwingung, Nachrichtensuche und detaillierten Konversationsprotokollen
- Echtzeit-Berichterstellung mit interaktiven Dashboards und Detailberichten

Die hochentwickelte Architektur ermöglicht hohe Leistung.

- Asynchrone, arbeitsspeicherbasierte Scans
- Integrierte Cluster-Funktionen und Lastausgleich für Hochverfügbarkeit
- Der standardmäßig enthaltene und stark skalierbare McAfee Quarantine Manager bietet gemeinsame Quarantänedienste für mehrere McAfee Email Gateway-Appliances sowie benutzerdefinierte Quarantänelisten und übernimmt Speicher- sowie Verarbeitungsaufgaben für bis zu 1,5 Millionen Nachrichten und bis zu 200.000 Benutzer

Zertifizierungen und Unterstützung

- Zertifizierung nach Common Criteria EAL2+, einschließlich NDPP-Compliance (Network Device Protection Profile)
- Software-Validierung und Zertifizierung für FIPS 140-2 Level 1
- Unterstützt Zugangskarten (x.509)
- Unterstützt IPv6

Einfach und zukunftssicher – vollständiger E-Mail-Schutz für jedes Unternehmen

Flexibler Einsatz

McAfee Email Gateway kann als Hardware-Appliance (in vier Appliance-Größen), virtuelle Maschine oder als Blade-Server-Architektur bereitgestellt werden. Diese Flexibilität ermöglicht erschwinglichen Schutz und Skalierbarkeit für anspruchsvollste Umgebungen zum geschäftlichen Nachrichtenaustausch. Zudem ist McAfee Email Gateway im Lieferumfang von McAfee Email Protection enthalten. Diese E-Mail-Sicherheitslösung kann wahlweise als E-Mail-Gateway vor Ort (als virtuelle oder Hardware-Variante), als Cloud-basierter SaaS (Security-as-a-Service) oder als Hybrid-Variante eingesetzt werden, wobei lediglich ein gemeinsamer Abonnementpreis anfällt.

Unternehmen, die den Vorteil der Cloud nutzen möchten, dabei jedoch auf die Kontrolle vor Ort Wert legen, können die integrierte Hybrid-Lösung einsetzen, bei der McAfee Email Gateway als Kontrollzentrum für die Cloud-basierte und Vor-Ort-Verwaltung von Richtlinien, gemeinsame Berichterstellung, Nachrichtensuche und Quarantäne zum Einsatz kommt. Üblicherweise wird die Hybrid-Variante in Unternehmen eingesetzt, die gefährliche oder lästige Inhalte vom eigenen Netzwerk fernhalten, die benötigte Bandbreite reduzieren und die Verwaltung sowie Verschlüsselung sensibler Informationen auf einer Vor-Ort-Appliance übernehmen möchten.

Security Connected

Das Security Connected-Framework unterstützt Kunden bei der Verbesserung ihrer Sicherheitslage, bei der Optimierung der Kosteneffizienz von Sicherheitsmaßnahmen sowie bei der strategischen Anpassung der Sicherheit an Unternehmensinitiativen. Durch die Integration in die Software McAfee ePO wird die Verwaltung und Berichterstellung innerhalb sowie über verschiedene Sicherheitslösungen hinweg vereint. McAfee Global Threat Intelligence (McAfee GTI) nutzt das gesamte Portfolio an McAfee-Lösungen und erfasst gesammelte Informationen aus jedem Bedrohungsvektor, der von unseren Lösungen abgedeckt wird. Die korrelierten Daten und Informationen werden anschließend an unsere Produkte und Lösungen übermittelt. Auf diese Weise ist gewährleistet, dass sich die E-Mail-Sicherheit von McAfee, als Bestandteil von Intel Security, auf die neuesten und aktuellsten Zero-Hour-Informationen verlassen kann. McAfee Advanced Threat Defense erkennt aktuelle verborgene Zero-Day-Malware und integriert sich nahtlos in verschiedene Produkte wie McAfee Email Gateway. McAfee Advanced Threat Defense kann von mehreren Ressourcen gemeinsam genutzt werden, sodass die Lösung effektiv für das gesamte Netzwerk skaliert werden kann und gleichzeitig die Betriebskosten sinken.

Sie erhalten unternehmensgerechte Funktionen, die sich für größte und anspruchsvollste Anforderungen skalieren lassen – bei minimalem Verwaltungs- und Kostenaufwand. Die einzigartige Kombination aus Funktionalität, Leistung, Zuverlässigkeit und Nutzen hat McAfee Email Gateway zur bevorzugten Lösung für die E-Mail-Sicherheit in mehr als der Hälfte der Fortune 500 IT-Unternehmen gemacht. Weitere Informationen über McAfee E-Mail Gateway-Lösungen finden Sie unter **www.mcafee.com/de/products/email-and-web-security/email-security.aspx**.

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