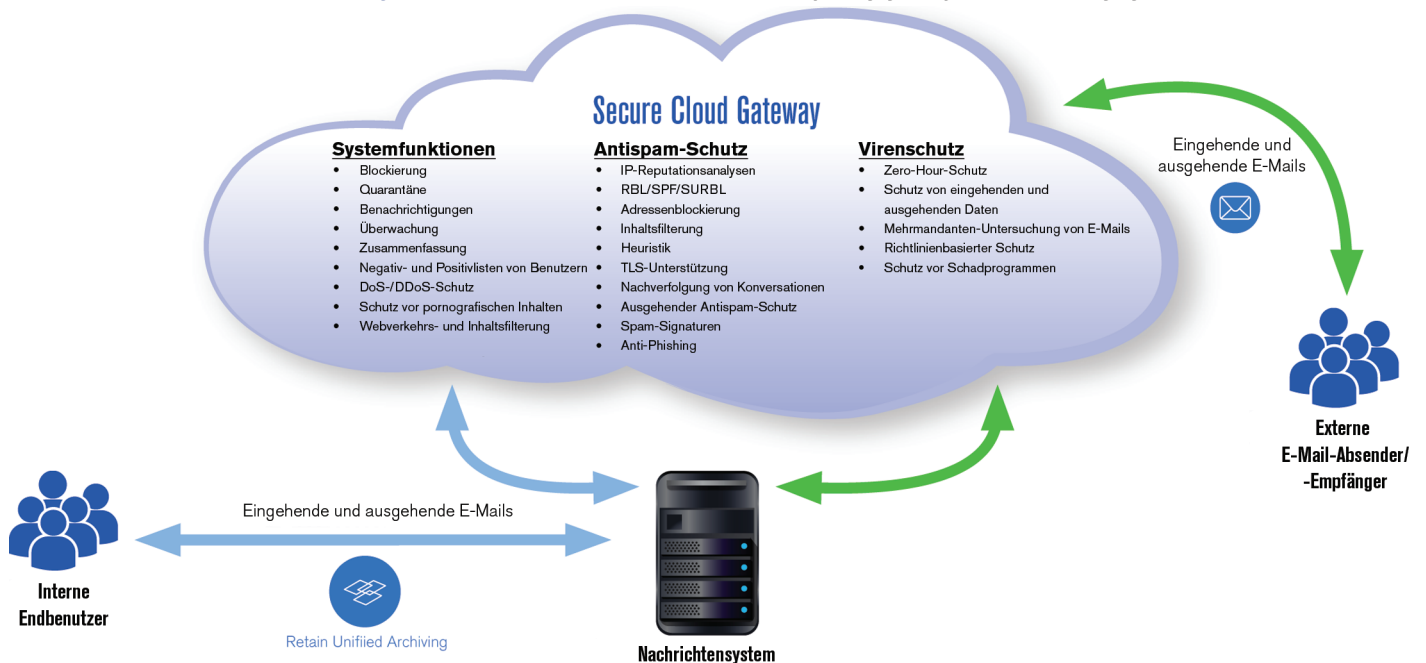


Micro Focus Secure Cloud Gateway

Micro Focus Secure Cloud Gateway bietet einen signatur-basierten Zero-Hour-Antiviren- und Anti-Spam-Schutz in der Cloud. Diese Lösung nutzt neueste Technologien, um sicherzustellen, dass Ihr Nachrichtensystem sowie Ihr Netzwerk frei von Viren, Schadprogrammen und Spam sind. Secure Cloud Gateway überwacht zudem den Netzwerkverkehr und blockiert pornografische Bilder sowie den Zugriff auf bösartige Websites und Inhalte und schützt vor Internetkriminalität und DoS- oder DDoS-Angriffen.

Nachrichtenverarbeitung: Durch einen einfachen DNS-Wechsel kann Secure Cloud Gateway Messaging Security dem SMTP-Flow hinzugefügt werden



Produkthighlights

Micro Focus wird bei Tausenden von Organisationen auf der ganzen Welt in Behörden, in Bildungseinrichtungen, in der Finanzdienstleistungsbranche, im Gesundheitswesen sowie in privatwirtschaftlichen Unternehmen zum Schutz von Unternehmensnetzwerken und Kommunikationsdaten eingesetzt.

Produktmerkmale

Unterstützung für mehrere Systeme: Micro Focus Secure Cloud Gateway kann Nachrichten am Netzwerkrand jedes standardbasierten Internet-E-Mail- oder Collaboration-Systems filtern. Dies umfasst Plattformen wie Microsoft Exchange, Office 365, Gmail, Micro Focus GroupWise, Vibe, Lync oder Lotus Domino.

Rollenbasierte Benutzerverwaltung:

Gewähren Sie Ihren Benutzern einen bestimmten rollenbasierten Zugriff direkt in Secure Cloud Gateway. Mit der neuen Zugriffssteuerungsliste können Sie den Benutzerzugriff auf Merkmale und Funktionen von Secure Cloud Gateway basierend auf den von Ihnen festgelegten Rollen verwalten. Aufgeführte Benutzer können nun Zugriff auf

bestimmte Verwaltungsfunktionen erhalten, ohne vollständige Administratorrechte besitzen zu müssen.

Skalierbares Design: Wenn Ihr System langsam seine Kapazitätsgrenze erreicht oder unter hoher Belastung arbeitet, können Sie neue Ressourcen (zusätzliche Secure Cloud Gateway-Server) zum Ausgleich der Last in Ihrem Micro Focus System hinzufügen.

Fehlertolerante Konfiguration: Secure Cloud Gateway kann auf mehreren Servern eingerichtet werden. Dadurch kann Ihr System weiterhin ausgeführt werden, auch wenn ein oder mehrere Server ausfallen.

Einfach zu konfigurierende, anpassbare Ad-Hoc-Benachrichtigungen: Erstellen Sie spezielle Benachrichtigungen, die Sie haben möchten oder brauchen. Die Arten von Benachrichtigungen, die Sie erstellen können, sind nahezu unbegrenzt. Sie können durch Schlüsselwörter, Anlagen, Inhalte, verbotene Bilder, Viren, Spam und andere Elemente ausgelöst werden. Zudem können alle Benachrichtigungen lokalisiert werden, sodass Sie die von Micro Focus generierten lokalisierten Versionen aller E-Mails bereitstellen können.

Antivirenschutz

Zero-Hour-Schutz: Secure Cloud Gateway bietet den besten Zero-Hour-Antivirenschutz, der für eingehenden und ausgehenden Datenverkehr verfügbar ist. Viren werden gestoppt, bevor sie Unheil anrichten, sodass Sie Tausende Dollar für Zeit- und Datenverlust sparen.

Schutz von eingehenden und ausgehenden Daten: Viren und Schadprogramme sind Bedrohungen, die von einer Vielzahl von Einstiegspunkten in Ihr Netzwerk eindringen können. Durch die Untersuchung ein- und ausgehender Daten bietet Secure Cloud Gateway einen einzigartigen Schutz, durch den sichergestellt ist, dass Bedrohungen und Schäden minimiert werden.

Richtlinienbasierte Mehrmandanten-Konfiguration: Micro Focus ermöglicht

das Erstellen und Konfigurieren von einzelnen Nachrichten-Richtlinien auf Basis der Sendeinformationen der einzelnen Nachrichten. Verwenden Sie Kriterien wie den Empfänger, die Quelladresse und die Nachrichtenrichtung zum Erstellen von einzelnen Nachrichten-Richtlinien für eingehende und ausgehende E-Mails, für einzelne Benutzer, Domänen oder mehrere Sätze von Benutzern. Secure Cloud Gateway unterstützt zudem eine volle Mehrmandanten-Untersuchung von E-Mails über einzelne Messaging-Gateways. In Verbindung mit der regelbasierten Steuerung können Micro Focus Partner und Dienstleister Messaging Security als gehostete Lösung nutzen.

Antiviren-Untersuchungen: Secure Cloud Gateway sucht nach Viren in der Betreffzeile, im Nachrichtentext und in den Anhängen einer E-Mail. Wenn der Anhang ein Virus enthält, wird die E-Mail-Nachricht am Gateway gestoppt. Darüber hinaus wird die E-Mail blockiert, wenn der Nachrichtentext oder die Betreffzeile der E-Mail einen schädlichen Link oder ein Virus enthält.

Leistungsstarke Multi-Thread-Untersuchungen: Stellen Sie mit asynchronen Thread-Untersuchungen über alle verfügbaren Ressourcen auf dem Server einen leistungsstarken Schutz Ihrer E-Mails sicher.

Musterabgleich: Secure Cloud Gateway unterstützt standardbasierte reguläre Ausdrücke für den Musterabgleich. Zudem ermöglicht Micro Focus das Anwenden von Mustern und die Untersuchung der vollständigen Domäne. Beispiel: Bei der Suche nach Mustern in E-Mail-Inhalten wird *companydomain.com für alle E-Mail-Adressen angewendet, die diese Domäne verwenden.

Antispam-Schutz

Schutz auf mehreren Ebenen: Secure Cloud Gateway bietet einen mehrschichtigen Antispam-Schutz für E-Mails und hält unerwünschten Datenverkehr von Ihrem Collaboration-System fern.

Perimetersicherheits-Untersuchung: Die Secure Cloud Gateway Soft-Appliance

für Spam am Netzwerkrand fängt Spam ab, bevor er Ihr Nachrichtensystem erreicht. Die Spam-Blockier-Funktionen umfassen Adressenblockierung, Filterung von Inhalten, Heuristik, SURBL-Technologie, IP-Reputationsanalysen, Nachverfolgung von Konversationen und TLS-Unterstützung. Durch die Eliminierung von Spam sorgt Micro Focus dafür, dass Ihr E-Mail-System reibungslos und effizient läuft.

Minimierung von falsch-positiven Ergebnissen: Die Antispam-Engine wird ständig mit neuen Spam-Signaturen aktualisiert. Diese innovative Technologie gewährleistet, dass falsch-positive Ergebnisse erkannt werden. Die E-Mails, die Sie benötigen, landen in Ihrem Posteingang, und nur Spam wird herausgefiltert.

Zuverlässige Inhaltsfilterung: Secure Cloud Gateway filtert E-Mail-Inhalte auf Basis von E-Mail-Adresse, Betreff, Header, Textkörper, Raw-MIME, Fingerabdruck, Anlagen, Anlagenamen, Bildern (über Image Analyzer), Negativ- und Positivlisten, Nachrichtengröße und IP-Adresse.

Direktionale Filterungssteuerung: Mit Micro Focus können Sie Filter basierend auf der Nachrichtenrichtung (Filter für ausgehende bzw. eingehende Nachrichten) erstellen. Sie können für eingehenden Datenverkehr andere Filter anwenden als für ausgehenden Datenverkehr.

Umschlag-Filterung: Mit Secure Cloud Gateway können Sie Filter basierend auf der Authentifizierung von Benutzern erstellen. Wenn ein im System authentifizierter Benutzer eine E-Mail sendet, kann das System diese Nachricht in einer bestimmten Weise verarbeiten. Zum Beispiel kann Secure Cloud Gateway Nachrichten von einem Benutzer blockieren, der nicht authentifiziert ist.

Ausgehender Antispam-Schutz: Workstations von Endbenutzern können mit Viren infiziert werden, die die Perimetersicherheit durchdringen. Diese Workstations können dann den Spam über Ihr Netzwerk verteilen und das System zu einer Quelle für Tausende

von ausgehenden Spam-Nachrichten machen. Secure Cloud Gateway eliminiert Risiken durch ausgehende Spam-Nachrichten, einschließlich einer blockierten IP-Adresse, Reputationsverlust, Verlust von Ressourcen und lahmgelegter Nachrichtensysteme.

Anti-Spoofing mit SPF-Untersuchung:

Zur Vermeidung von E-Mail-Spoofing führt Secure Cloud Gateway eine Sender Policy Framework (SPF)-Untersuchung durch. SPF prüft die Domäne, die im Absenderbereich der MIME-Datei zu finden ist, und überprüft dann die SPF-Datensätze dieser Domäne, um sicherzustellen, dass die Domäne, die die E-Mail berichtet, den Mailservern entspricht, die die Domäne senden. Durch SPF kann Secure Cloud Gateway basierend auf in einer Absenderrichtlinie des Domänen-Anbieters veröffentlichten Informationen Nachrichten identifizieren, die autorisiert bzw. nicht autorisiert sind, den Domänennamen in den Befehlen „SMTP-HELO“ und „MAIL FROM“ zu verwenden.

Schutz des Netzwerks

Schutz vor Cyberkriminalität: Cyberkriminalität, Cyberterrorismus und Schadprogramme sind ernste Bedrohungen für Ihr Unternehmen. Micro Focus bietet spezielle Schutzmaßnahmen auf mehreren Ebenen, damit Cyberkriminelle Ihre Infrastruktur nicht per E-Mail angreifen können.

Schutz vor pornografischen Inhalten:

Zur genauen Erkennung untersucht Micro Focus Image Analyzer die Zusammensetzung von Bildern und Videos. Die ausgefeilte Wahrscheinlichkeits-Engine untersucht eingehende und ausgehende Bilder, unterscheidet zuverlässig zwischen pornografischen und nicht-pornographischen Inhalten und stoppt unangemessene Inhalte vor dem Eingang in bzw. vor dem Ausgang aus Ihrem Nachrichtensystem.

DoS- oder DDoS-Schutz:

Verhindern Sie Denial-of-Service (DoS)- und Distributed DoS (DDoS)-Angriffe auf die SMTP, die Ihren Mail-Server lahmlegen können. Dies führt zu Systemausfällen und Ausfallzeiten und kostet Ihr Unternehmen Zeit und Geld in Form von verlorener Produktivität.

Negativ- und Positivlisten von Benutzern:

Geben Sie Benutzern mehr Rechte, und verringern Sie dadurch Verwaltungsaufwand und -kosten. Secure Cloud Gateway bietet eine Benutzeroberfläche, mit der Benutzer Domänen und E-Mail-Adressen kennzeichnen können. Die Benutzer können einzelne E-Mail-Adressen oder komplette Domänen auf ihre Negativ- und Positivlisten setzen, so dass Meldungen auf Grundlage dieser Liste empfangen oder blockiert werden.

Vorteile der Cloud

Cloud-Funktionen: Dank der Mehrmandantenfähigkeit von Micro Focus können

mehrere unabhängige Instanzen der Scan-Konfigurationen auf demselben Server ausgeführt werden. So können Sie alle Funktionen von Secure Cloud Gateway nutzen und gleichzeitig Support für eine Vielzahl von Kunden über ein System bieten. Die Cloud-Lösung sichert Ihr Nachrichtensystem ohne die zusätzlichen Kosten und Risiken sowie ohne den zusätzlichen Aufwand in Zusammenhang mit einem lokalen Messaging Security System. Überlassen Sie die IT-, Hardware- und Supportkosten Micro Focus.

Schnelle Bereitstellung: Verringerung der Implementierungskosten durch einfache Bereitstellung per Verweis Ihrer Nachrichtenserver auf Secure Cloud Gateway.

Vordefinierte Sicherheitspakete: Verwenden Sie die voreingestellten Regeln von Secure Cloud Gateway für maximalen Schutz. Die Regeln können zudem angepasst werden, um Ihre spezifischen Anforderungen zu erfüllen.

Vielfach preisgekrönter Support: Die Micro Focus Cloud umfasst den Zugriff auf zertifizierte Techniker – 24 Stunden am Tag, sieben Tage die Woche.

Skalierbarer Zugriff: Verwenden und bezahlen Sie nur den Service, den Sie brauchen. Die Micro Focus Cloud bietet On-Demand-Verfügbarkeit von Server und Netzwerkauslastung.

„Wenn ich (externen Administratoren) erzähle, wie viel Spam wir pro Monat mit Micro Focus Secure Gateway blockieren, können sie es kaum glauben.“

ROY DRAGOTTA
Network Engineer
Long Island Rail Road

www.microfocus.com



**Micro Focus
Deutschland**

Fraunhoferstraße 7
D-85737 Ismaning
00 800-58102130

**Micro Focus
Schweiz**

Merkurstrasse 14
8953 Dietikon
Switzerland
00 800-58102130

**Micro Focus
Firmenhauptsitz**

Vereinigtes Königreich
+44 (0) 1635 565200

www.microfocus.com