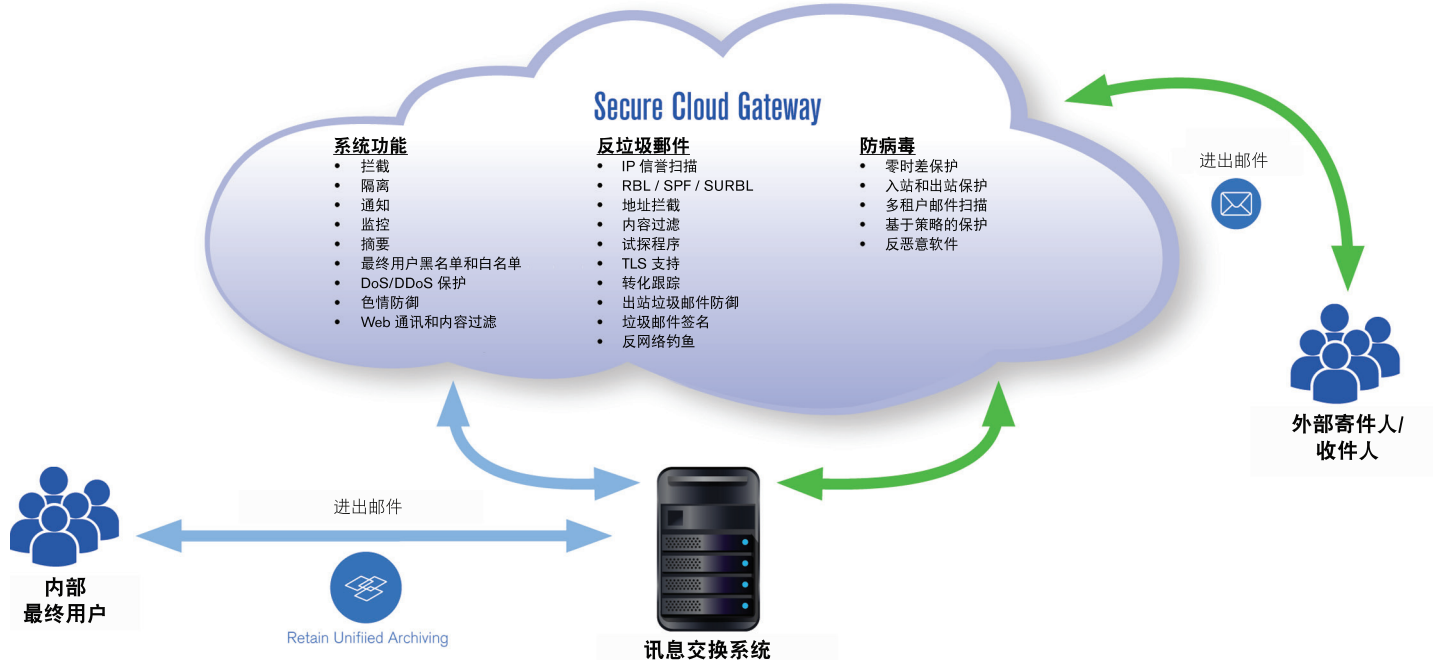


Micro Focus Secure Cloud Gateway

Micro Focus® Secure Cloud Gateway 在云端提供基于签名的“零时差”防病毒和反垃圾邮件保护。该解决方案使用最新技术确保讯息系统和网络远离病毒、恶意软件和垃圾邮件。Secure Cloud Gateway 还能监视网络通讯以屏蔽淫秽图像，阻止访问恶意网站和内容，并防范网络犯罪和 DoS 或 DDoS 攻击。

讯息处理：简单的 DNS 更改即可将 Secure Cloud Gateway 讯息交换安全功能融入 SMTP 流程中



产品亮点

Micro Focus 为全球成千上万个组织保护业务网络和通信数据，覆盖政府、教育、商业、金融服务、医疗保健等众多行业。

产品功能

多系统支持：Micro Focus Secure Cloud Gateway 可以在任何基于标准的因特网邮件系统或协作系统的外围过滤讯息。其中包括 Microsoft Exchange、Office

365、Gmail、Micro Focus GroupWise®、Vibe、Lync 或 Lotus Domino 等平台。

基于角色的用户管理：在 Secure Cloud Gateway 中授予用户基于角色的特定访

问权限。使用全新的访问控制列表，您可以根据设定的角色来管理用户对 Secure Cloud Gateway 功能的访问权限。指定用户现在可以访问某些管理功能，不必具有完整的管理权限。

可缩放设计：当您的系统接近能力上限，或者面临运行压力时，您能够添加新资源（额外的 Secure Cloud Gateway 服务器）来平衡 Micro Focus 系统上的负载。

容错配置：Secure Cloud Gateway 可以安装在多台服务器上。即使一台或多台服务器出现故障，您的系统仍然保持正常运行。

容易配置的特定自定义通知：创建您想要或需要的特定通知。您可以创建的通知类型几乎是不受限制的。关键字、附件、内容、病毒、违法图像、垃圾邮件等都能触发通知。此外，所有通知都可以本地化，因此您可以为 Micro Focus 系统生成的所有邮件提供本地化版本。

病毒防护

零时差防护：Secure Cloud Gateway 为入站和出站通讯提供最佳的零时差病毒保护。病毒在爆发之前就被拦截下来，避免了数千美元的时间和数据损失。

入站和出站保护：病毒和恶意软件会从各种入口侵入您的网络。Secure Cloud Gateway 凭借入站和出站扫描为您提供独特防护，确保威胁和损失降至最低限度。

基于策略的多租户配置：Micro Focus 让您能够根据每条消息的递送信息创建和配置单独的讯息策略。它使用收件人、源地址和传送方向等指标为单个用户、多组用户或域的进出邮件创建单独的讯息策略。Secure Cloud Gateway 还支持通过讯息交换专用网关进行全面的多租户邮件扫描。如果与基于策略的控制功能结合使用，讯息安全功能可以作为 Micro Focus 合作伙伴和服务提供商的托管解决方案。

防病毒扫描：Secure Cloud Gateway 可扫描电子邮件的主题、正文和附件。如果附件含有病毒，电子邮件消息将被阻止在网关位置。此外，如果电子邮件的正文或主题含有恶意链接或病毒，电子邮件将被拦截。

多线程高性能扫描：针对服务器上所有可用资源，异步线程化多个扫描进程，实现高性能邮件扫描。

模式匹配：Secure Cloud Gateway 支持基于标准的模式匹配正则表达式。此外，Micro Focus 还允许您为整个域应用模式和扫描。例如，*companydomain.com 将应用到使用该域的所有邮件地址，以搜索邮件内容中的模式。

反垃圾邮件保护

多层防御：Secure Cloud Gateway 提供多层垃圾邮件防护，让无关的通讯远离您的协作系统。

外围防御：Secure Cloud Gateway 软设备专门在外围抵御垃圾邮件，能在垃圾邮件到达讯息系统之前将其捕获。垃圾

邮件拦截功能包括：地址拦截、内容过滤、试探程序、SURBL 技术、IP 信誉扫描、转化跟踪和 TLS 支持。通过杜绝垃圾邮件，Micro Focus 能使您的邮件系统实现高效、平稳的运行。

最大限度减少误报：反垃圾邮件引擎不断通过新的垃圾邮件签名进行更新。这种创新技术确保检测到误报情况。您需要的邮件终将到达收件箱，只会过滤出垃圾邮件。

强大的内容过滤：Secure Cloud Gateway 根据电子邮件的地址、主题、标题、正文、原始 MIME、指纹、附件、附件名称、图像（利用 Image Analyzer）、黑名单或白名单、讯息大小和 IP 地址来过滤邮件内容。

定向过滤控制：Micro Focus 支持您基于讯息方向创建过滤器（出站和进站过滤器）。您可以为进站通讯和出站通讯应用不同的过滤器。

封套过滤：Secure Cloud Gateway 允许您根据用户身份的鉴定进行过滤。如果用户在系统中进行鉴定，则发送邮件讯息时，该解决方案能以指定方式处理该讯息。例如，Secure Cloud Gateway 可以拦截未获鉴定的用户发送的讯息。

出站垃圾邮件防御：最终用户工作站可能会被穿过外围防御的病毒侵袭。这些工作站随后会借助您的网络推送垃圾邮件，将您的系统变为数千封出站垃圾邮件的来源。Secure Cloud Gateway 有助于规避出站垃圾邮件风险，比如 IP 地址受阻、声誉受损、资源损失、讯息系统损坏。

SPF 扫描反欺骗：为了阻止电子邮件欺骗，Secure Cloud Gateway 增添了“发件人策略框架”（SPF）扫描功能。SPF 首先查看 MIME 文件“发件人”部分含有的域，然后检查该域的 SPF 记录，以确保邮件报告的域与发送该域的邮件服务器匹配。Secure Cloud Gateway SPF 功能可以根据域拥有者在发件人策略中发布的信息，识别出获准或未获准在 SMTP HELO 和 MAIL FROM 命令中使用域名的讯息。

网络保护

抵御网络犯罪：网络犯罪、网络恐怖主义和恶意软件会严重威胁您的组织。Micro Focus 提供多层专门防护，使得网络罪犯无法利用电子邮件作为攻击基础设施的方法。

色情防御：Micro Focus Image Analyzer 扫描图片和视频的实际内容，确保符合要求。先进的概率引擎可以扫描进出的

图片，明确区分色情和非色情内容，以及阻止不当内容进入或离开讯息系统。

DoS 或 DDoS 保护：防止“拒绝服务”（DoS）和“分布式 DoS”（DDoS）攻击 SMTP，从而避免邮件服务器瘫痪。否则会导致系统中断和停机，使贵组织因为生产力丧失而产生时间和金钱成本。

最终用户黑名单和白名单：赋予最终用户权限，减少管理时间和成本。Secure Cloud Gateway 为最终用户提供了一个用于标记域和邮件地址的界面。最终用户可以将单个邮件地址或整个域添加到黑名单或白名单，然后根据名单拦截或放行讯息。

云优点

云功能：Micro Focus 这款产品具有多租户支持功能，能在同一服务器上运行多个独立的扫描配置实例。这让您既享有 Secure Cloud Gateway 的全部功能，又

可利用一个系统支持多个客户。云解决方案在保护您的讯息系统的同时，不会像就地讯息安全系统那样引入额外的成本、风险和复杂性。让 Micro Focus 帮您节省 IT、硬件和系统的支持成本吧。

快捷部署：您的讯息交换服务器直接指向 Secure Cloud Gateway 即可投入运行，节约了实施成本。

预定义保护包：使用 Secure Cloud Gateway 的预设规则实现最佳保护。此外，您可以根据特定需要自定义这些规则。

屡获殊荣的支持：Micro Focus 云支持您全天候联系获得认证的技术人员。

可缩放式访问：按需使用服务，并支付相应费用。Micro Focus 云按需供应服务器和网络资源。

“当我告诉外部管理员我们使用 **Micro Focus Secure Gateway** 每月拦截了多少垃圾邮件时，他们难以置信。”

ROY DRAGOTTA

网络工程师
长岛铁路公司

www.microfocus.com



班加罗尔

+91 80 4002 2300

北京

+86 10 6533 9000

广州

+86 20 3877 1892

香港

+852 3978 2339

马来西亚

+60 3761 00214

上海

+86 21 6062 6267

深圳

+86 755 8282 2655

Micro Focus

英国总部

+44 (0) 1635 565200

www.microfocus.com