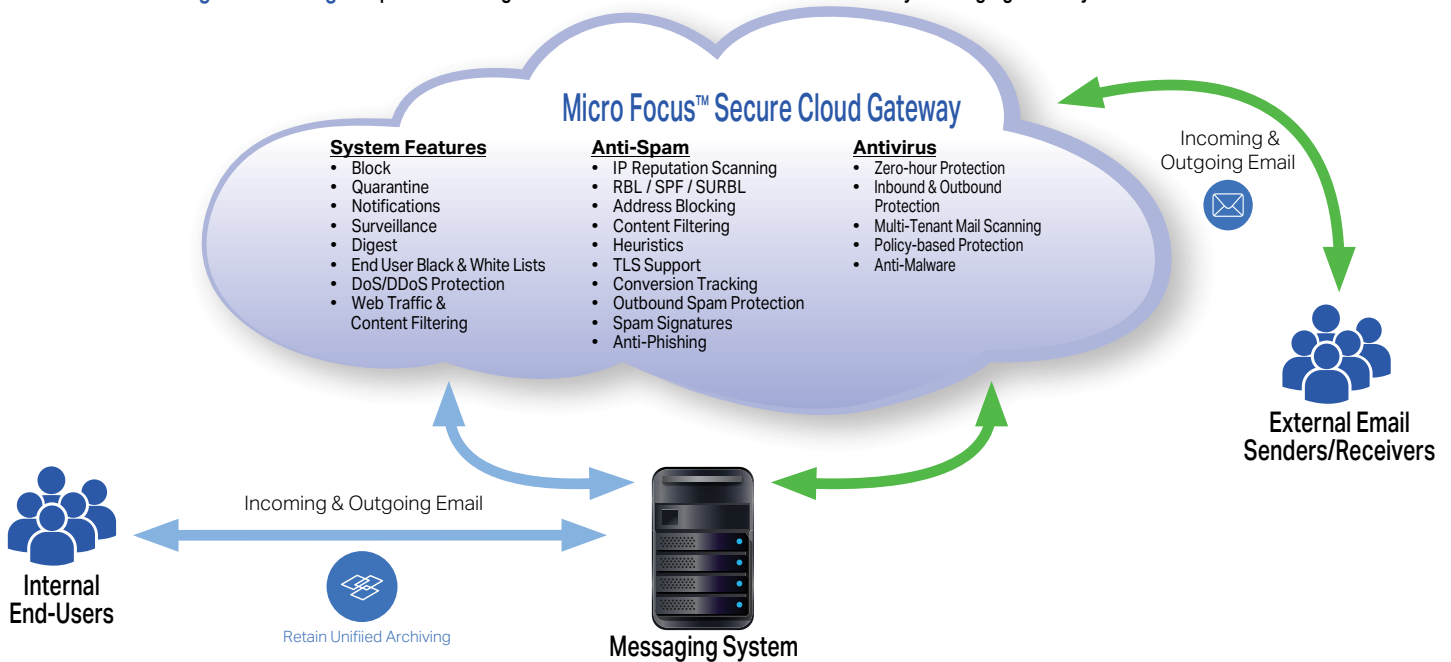


Secure Cloud Messaging Gateway

Micro Focus™ Secure Cloud Messaging Gateway provides signature-based, zero-hour antivirus and anti-spam protection in the cloud. This solution uses the latest technology to ensure that your messaging system and network are free of viruses, malware, and spam. Micro Focus™ Secure Cloud Messaging Gateway also protects from DoS/DDoS attacks helping to keep your email system up and running.

Message Processing: Simple DNS Change Inserts Micro Focus™ Secure Cloud Gateway Messaging Security into the SMTP Flow



Product Highlights

OpenText™ protects business networks and communication data for thousands of organizations around the world in industries including government, education, financial services, healthcare, and business.

Product Features

Multi-System Support: Micro Focus™ Secure Cloud Messaging Gateway by OpenText™ can filter messaging at the perimeter of any standards-based internet mail or collaboration system. This includes platforms such as

Microsoft Exchange, Office 365, Gmail, and OpenText™ GroupWise.

Role-Based User Administration: Grant your users specific role-based access within Micro Focus™ Secure Cloud Messaging Gateway.

The new Access Control List allows you to manage user access to features and functions of Micro Focus™ Secure Cloud Messaging Gateway, based on the roles you set. Named users can now have access to certain administration features without having full administration rights.

Scalable Design: When your system starts to reach capacity or is under strain, you are able to add new resources (additional Micro Focus™ Secure Cloud Messaging Gateway servers) to balance the load on your OpenText system.

Fault Tolerant Configuration: Micro Focus™ Secure Cloud Messaging Gateway can be set up on multiple servers. This allows your system to continue to run, even if one or more servers goes down.

Easy-to-Configure, Ad-Hoc, Customizable Notifications: Create the specific notifications you want or need. The types of notifications you can create are almost limitless. They can be triggered by keywords, attachments, content, viruses, spam, and other categories. Plus, all notifications can be localized, allowing you to provide localized versions of all of the emails that OpenText generates.

Antivirus Protection

Zero-Hour Protection: Micro Focus™ Secure Cloud Messaging Gateway provides the best zero-hour antivirus protection available for both inbound and outbound traffic. Viruses are stopped before an outbreak occurs, which saves you thousands of dollars in lost time and data.

Inbound and Outbound Protection: Viruses and malware are threats that can penetrate your network from a wide range of entry points. With inbound and outbound scanning, Micro Focus™ Secure Cloud Messaging Gateway provides unique protection, ensuring that threats and damages are minimized.

Policy-Based, Multi-Tenant Configuration:

OpenText lets you create and configure individual message policies based on the delivery information of each individual message. Use criteria such as the recipient, the source address, and direction to create separate message policies for incoming and outgoing email, for individual users, domains, or multiple sets of users. Micro Focus™ Secure Cloud Messaging Gateway also supports full multi-tenant mail scanning through single-messaging gateways. Combined with the policy-based control, OpenText partners, and service providers can use Messaging Security as a hosted solution.

Anti-Virus Scanning: Micro Focus™ Secure Cloud Messaging Gateway scans for viruses in the subject, body, and attachments of an email. If the attachment contains a virus, the email message will be stopped at the gateway. Plus, if the body or subject of the email contains a malicious link or a virus, the email is blocked.

Multi-Threaded, High-Performance Scanning:

Enable high-performance email scanning by threading scan processes asynchronously across all available resources on the server.

Pattern Matching: Micro Focus™ Secure Cloud Messaging Gateway supports standards-based regular expression for pattern matching. Plus, OpenText allows you to apply patterns and scanning to the full domain. For example, *companydomain.com will be applied to all email addresses using that domain, to search for patterns in email content.

Anti-Spam Protection

Multilayer Defense: Micro Focus™ Secure Cloud Messaging Gateway provides multilayer spam defense to protect email and keep unwanted traffic away from your collaboration system.

Perimeter Defense Scanning: The Micro Focus™ Secure Cloud Messaging Gateway soft appliance, for spam at the perimeter, catches spam before it ever reaches your

messaging system. Spam-blocking functions include address blocking, content filtering, heuristics, SURBL technology, IP reputation scanning, conversion tracking, and TLS support. By eliminating spam, OpenText keeps your email system running smoothly and efficiently.

Minimize False-Positives: The anti-spam engine is constantly updated with new spam signatures. This innovative technology assures that false-positives are detected. The mail you need ends up in your inbox, and only spam gets filtered out.

Robust Content Filtering: Micro Focus™ Secure Cloud Messaging Gateway filters email content based on email address, subject, header, body, Raw MIME, fingerprinting, attachment, attachment names, images (via Image Analyzer), black-list or white-list, message size, and IP address.

Directional Filtering Control:

OpenText allows you to create filters based on message direction (outbound versus inbound filters). Apply different filters to inbound traffic than you would for outbound traffic, and vice versa.

Envelope Filtering: With Micro Focus™ Secure Cloud Messaging Gateway, you can filter based on authentication of users. If a user is authenticated in the system and they send an email message, the solution can deal with that message in a specified way. For example, Micro Focus™ Secure Cloud Messaging Gateway can block messages from a user that is not authenticated.

Outbound Spam Protection: End-user workstations can become compromised by viruses that penetrate perimeter defenses. Those workstations can then push spam out through your network, turning your system into a source for thousands of outbound spam. Micro Focus™ Secure Cloud Messaging Gateway helps prevent outbound spam risks including blocked IP address, damaged reputation, loss of resources, and crippled messaging systems.

“When I tell (outside administrators) how much spam we block per month with [Micro Focus™] Secure Cloud Messaging Gateway, they can’t believe it.”

ROY DRAGOTTA
Network Engineer
Long Island Rail Road

Connect with Us



Anti-Spoofing with SPF Scanning: To stop email spoofing, Micro Focus™ Secure Cloud Messaging Gateway features Sender Policy Framework (SPF) scanning. SPF looks at the domain found in the ‘mail from:’ part of the mime file, then checks that domain’s SPF records to make sure that the domain that the email is reporting matches the mail servers that send that domain. SPF allows Micro Focus™ Secure Cloud Messaging Gateway to identify messages that are or are not authorized to use the domain name in the SMTP HELO and MAIL FROM commands, based on information published in a sender policy of the domain owner.

Network Protection

Cybercrime Protection: Cybercrime, cyberterrorism, and malicious malware are serious threats to your organization. OpenText provides multiple layers of specialized protection to keep cybercriminals from using email as a method of attacking your infrastructure.

DoS or DDoS Protection: Prevent Denial of Service (DoS) and Distributed DoS (DDoS) attacks to the SMTP, which can take down your mail server. This leads to system outages and downtime, costing your organization time and money in lost productivity.

End-User Black and White Lists: Empower end users and reduce administration time and costs. Micro Focus™ Secure Cloud Messaging Gateway features an interface for end users to flag domains and email addresses. The end users can place individual email addresses or complete domains on their black or white list, allowing for messages to pass through or be blocked based on this list.

Cloud Benefits

Cloud Functionality: OpenText’s multi-tenant support enables multiple independent instances of scan configurations to run on the same server. It allows you to have all the functionality of Micro Focus™ Secure Cloud Messaging Gateway while supporting multiple customers from one system. The cloud solution secures your messaging system without the additional costs, risks, and complexity associated with an on-premises messaging security system. Let OpenText handle the IT, hardware, and system support costs.

Rapid Deployment: Reduce implementation costs by simply pointing your messaging servers to Micro Focus™ Secure Cloud Messaging Gateway and you are up and running.

Pre-defined Protection Packages: Use the Micro Focus™ Secure Cloud Messaging Gateway pre-set rules for maximum protection. Plus, these rules can be customized to meet your specific needs.

Award Winning Support: The OpenText cloud includes access to certified technicians 24 hours a day, seven days a week.

Scalable Access: Only use, and pay for, the service that you need. The OpenText cloud provides on-demand availability of server and network usage.

Learn more at
www.opentext.com