opentext™

Data Sheet

OpenText Secure Messaging Gateway

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

Product Highlights

OpenText™ Secure Messaging Gateway protects business networks and communication data for thousands of organizations around the world in industries including gov-

Inbound and Outbound Protection

OpenText Secure Messaging Gateway provides inbound and outbound protection for your company's enterprise network & messaging system, including antivirus, anti-spam, cybercrime protection, and DoS/DDoS protection.

Antivirus Protection

Zero-hour Antivirus Protection: OpenText Secure Messaging Gateway provides the best zero-hour antivirus protection available for ERWKLQERXQGDQGRXWERXQG WUDIILF9LUXVHV DUH stopped before an outbreak occurs, which saves you thousands of dollars in lost time and data.

Anti-Virus Scanning: OpenText Secure 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. If the body or subject of the email contains a malicious link, or a virus, the email is blocked by OpenText Secure Messaging Gateway.

Policy-Based, Multi-Tenant Configuration: OpenText Secure Messaging Gateway lets you FUHDWHDQG FRQ HLQGLYLGXDOPHVVDJHSROL - cies 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. It also supports full multi-tenant mail scanning through single-messaging gateways. Combined with the policy-based control, partners and service providers can use OpenText Secure Messaging Gateway as a hosted solution.

Inbound and Outbound Protection: 9LUXVHV and malware are threats that can penetrate your network from a wide range of entry points. With inbound and outbound scanning, OpenText Secure Messaging Gateway provides unique protection, ensuring that threats and damages are minimized.

Multi-threaded, High Performance Scanning: Enable high performance email scanning by threading scan processes asynchronously across all available resources on the server.

Pattern Matching: OpenText Secure Messaging Gateway supports standards-based regular expression for pattern matching, and it allows

> “With 60,000 external e-mail messages, 300,000 internal email messages a month [OpenText] Secure Messaging Gateway was the easy choice for the nuclear plant with the top security rating in the country. I do a virus scanning nightly on the entire system. Viruses used to be an issue, but with [OpenText] Secure Messaging Gateway, they’re not now.”
>
> LOU DONATO
> Network Administrator
> South Texas Nuclear

Envelope Filtering: OpenText Secure Mes-VDJLQJ *DWHZD\ DOORZVIRUÌOWHU EDVHG RQ authentication of users. If a user is authenticated in the OpenText system and they send an email message, It can deal with that message LQVSHFLÌHGZD\ ) RUH[DPSOHLWFDQDOORZDOO messages from that user to enter the system and OpenText Secure Messaging Gateway can block messages from a user that is not authenticated.

Anti-Spoofing with SPF Scanning: To stop HPDLOVSRRÌQJ 2SHQ7H[W 6HFXUH0HVVDJLQJ 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 OpenText Secure 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.

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

DoS/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. OpenText 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.

Total GroupWise Support

OpenText Secure Messaging Gateway provides total scanning for your OpenText GroupWise messaging platform. It intercepts all messages passing through GroupWise MTA, POA, GWIA, WebAccess, and GMS in real time to help ensure that they are free of viruses, spam, and malware.

GroupWise WebAccess: Because GroupWise WebAccess communicates directly with the SRVWRÌFH E\SDVVLQJWKH670DQGWKH 07$ communication done via WebAccess is unprotected and could directly infect the post ofÌFH 7RPDQDJH :HE$FFHVV 2SHQ7H[W 6HFXUH Messaging Gateway sits at the GroupWise WebAccess Gateway and filters unwanted content before the it reaches the system. For complete OpenText coverage, OpenText Secure Messaging Gateway also includes a 9HEHSOXJLQ

Added Protection for GroupWise Mobility Service: OpenText Secure Messaging Gateway scans all messages sent from mobile devices connected to the GroupWise Messaging Service, and stops viruses before they enter the GroupWise system. This allows organizations to ensure that mobile messages are secure and that viruses are not spread to internal GroupWise users.

OpenText Vibe Support: OpenText Secure Messaging Gateway scans all messages and XSORDGVSRVWHGWR9LEHDQG VWRSVYLUXVHVEH-fore they enter the network. This ensures that 9LEHLV VHFXUH DQGWKDWYLUXVHV DUHQRW VSUHDG to internal system users.

Learn more at
www.opentext.com