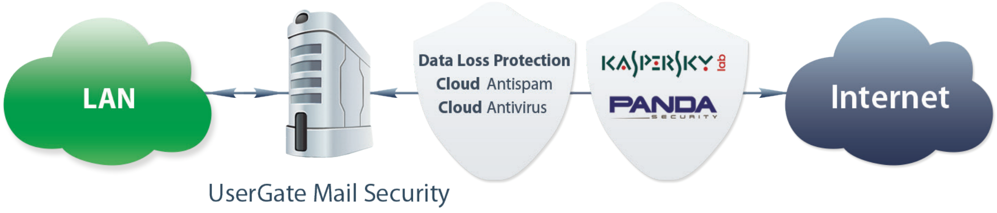
UserGate Mail Security

- ✓ **Antispam for Any Email Server**
- ✓ **Data Loss Protection (DLP)**
- ✓ **Email Archiving**
- ✓ **Secure and Protected Email**

Protect local network from viruses and spam

UserGate Mail Security is an antispam and antivirus solution that features integrated security software by most popular vendors and other mechanisms to make using emails safer and more comfortable.



Antispam for Any Email Server

UserGate Mail Security can provide top-level security and threat protection for any mail server so you can continue using all the features and functions of your current email server but benefit from additional security and monitoring features.

Our solution allows integrating with an IMAP server for MS Exchange and Lotus Domino. Due to its modular structure, UserGate Mail Security is highly efficient and failsafe.

Email Content Filtering and Data Leak Prevention

With UserGate Mail Security you can enforce the email content policy and provide enterprise-level protection against data theft and data loss for email.

Our solution carries out a series of strict checks on the incoming and outgoing email and intercepts messages based on the corporate policies enforced by the administrator.

Secure and Protected Email

The embedded AntiVirus and AntiSpam modules provide the best and broadest protection against new and zero-hour threats. A highly available cloud-based service hosted at multiple data centers ensures enhanced reliability and scalability.

UserGate Mail Security can protect against phishing, spear phishing, and targeted attacks and it can also scan links in emails to test if the sites contain malicious content. Due to our licensed Recurrent Pattern Detection technology,

UserGate Mail Security provides a typical sustained detection rate of more than 99%, with virtually zero false-positives (approximately 1 in 1.5 million).

Email Archiving

UserGate Mail Security can help you efficiently store, manage, and discover your organization's emails. It prevents data loss and provides for compliance with the relevant legal requirements.

About UserGate Mail security

UserGate Mail Security for Exchange Server/SMTP/Lotus is a solution for the protection of corporate email from viruses, phishing, spam and other malicious messages, that allows preventing confidential information leaks.

The product has options of messages backup and email account monitoring, supports synchronization with MS Exchange 2003 and Lotus Domino via IMAP, and can also operate with any other mail servers.

Due to its modular structure, UserWall Mail Security is highly efficient and failsafe. Antivirus and antispam cloud-based modules provide filtering of spam and viruses using a system of rapid response to new threats (Zero-Hour Protection) with almost no false response.

The average user in an organization of up to 1,000 employees sends and receives 124 emails on a typical workday; the average user in a larger organization sends and receives 149 emails each day.

Because 58% find email to be critical in getting their work done, and because other communication tools are becoming more widely used, attacks directed against these capabilities threaten the very ability of individuals and companies to communicate or protect their sensitive data.*

* "The Impact of Messaging and Web Threats", Osterman Research

entensys

www.entensys.com | sales@entensys.com

UserGate Mail Security

Antivirus and phishing protection

UserGate Mail Security uses three integrated antivirus modules: cloud-based Entensys Zero-Hour, Kaspersky and Panda antiviruses. A cloud-based antivirus enables proactive virus detection. Therefore, Entensys Zero-Hour begins fighting a new virus before it infects millions of computers.

Advantages of Cloud-Based Solution

Entensys Zero-Hour Antivirus does not require installing a large application that would take up most of your server's resources to run properly. The performance of the cloud-based antivirus module integrated in UserGate Mail Security only depends on your Internet channel's workload, in other words, the connection speed.

Early Virus Detection

Today, viruses, worms and Trojans are targeted for various vulnerabilities of antivirus solutions. The key constraint is the time required to create virus signatures or perform a heuristics analysis. Entensys jointly with the company security partners monitors the Web continuously to detect mass virus epidemics immediately as they break out. By using hundreds of servers (honeypots) located all over the world, Entensys is able to detect both spam and viruses. This approach enables proactive virus detection, allowing you to begin fighting a new virus before it infects millions of computers. That's why our solution is not based just on virus signatures, as is common for many other antivirus solutions.

Data Loss Protection (DLP)

UserGate Mail Security has the Data Loss Protection (DLP) module preventing confidential information leaks or penetration of other unwanted information from external sources.

Depending on the system settings, DLP module can prevent data losses by blocking or holding messages, or inform the Security Engineer of suspicious message sending. UserGate Mail Security uses three types of filtering: Regular expressions (Regexp), Documents matching (Docmatch) and a Lemmatizer. Each of them uses a different search method to scan body, threads, attachments and other parts of messages, to monitor Email messages for certain key words or phrases and to compare the transferred data with confidential information patterns.

Message backup

UserGate Mail Security allows you to backup incoming messages. The backup process is completed upstream of spam and virus filtering. You can specify the direction of messages to be backed up (incoming only, outgoing only or both) and list exception addresses in the Backup settings.

Cloud antispam

Cloud antispam filters messages based on their content and heuristics analysis. One of the main advantages of Entensys cloud antispam is a very low rate of false detections – less than one in 1.5 million messages, while its spam detection rate is over 97%.

Low False Response Level

One of the key merits of Entensys Cloud Antispam Module is a low false response level – less than one in 1.5 mln messages. At the same time, the spam detection rate is 97%. Traditional spam protection method based on IP and DNS black lists has a significantly higher occurrence of false response, while users that are not spammers are often added to black lists. This usually happens when a computer within a LAN is successfully attacked by spammers and later used to distribute spam messages.

Entensys Cloud Antispam Module sends to the cloud-based service a UID of a message, which helps define if the message contains spam, and further blocks this specific message or stops spam attack instead of blocking the IP address, domain or e-mail address. This feature of Entesys Antispam makes it useful for companies, where deletion of messages considered to be spam can cause loss of clients or other problems.

Monitoring and statistics

UserGate Mail Security provides information on all messages processed by the antispam solution server. UserGate Mail Security message monitoring allows filtering by date, processing status (delivered/blocked) or sender/recipient address, as well as push-sending messages blocked as spam, and creating exception lists.

IMAP integration

The Entensys solution features integration with an IMAP server for MS Exchange and Lotus Domino. Integration gives the opportunity to create a public IMAP folder on a remote mail server and process messages in these folders.

Additional methods of spam protection

When processed by UserGate Mail Security, messages go through several filtering stages, including connection filtering, sender filtering, recipient filtering and content filtering. In addition to cloud-based antispam requiring no user-specified settings, UserGate Mail Security supports the following additional filtering methods:

- based on DNS (DNSBL, RHSBL, Backscatter, MX, SPF, SURBL);
- based on a distributed antispam system (cloud antispam);
- based on statistical filtering (Bayesian filtering method designed by Entensys).

In addition, the solution supports SMTP monitoring (ensures the commands comply with RFC), allows to set the maximum message size, the maximum number of addressees, etc.