

UserGate Mail Security

Безопасность электронной почты от внешних и внутренних уязвимостей

UserGate Mail Security обеспечивает комплексную безопасность использования электронной почты в организации, используя одни из лучших в мире технологий по фильтрации спама и вирусов.



Антиспам для любого почтового сервера

UserGate Mail Security обеспечивает качественную защиту от угроз, связанных с электронной почтой, и работает с любыми почтовыми серверами. Таким образом, продукт позволяет полноценно использовать функционал того или иного почтового сервера и в тоже время получать все преимущества от использования дополнительных функций по безопасности и мониторингу.

Решение поддерживает синхронизацию по IMAP с MS Exchange и Lotus Domino. UserGate Mail Security обладает модульной структурой, это улучшает отказоустойчивость и повышает эффективность работы.

Защита от утечек персональных данных

UserGate Mail Security оснащен модулем защиты от потери данных (иначе DLP – Data Loss Protection), предотвращающим утечки конфиденциальной или другой нежелательной информации, а также проникновение ее извне.

В зависимости от настроек, система позволяет *блокировать, задерживать сообщения или оповещать* инженера безопасности об отсылке подозрительного письма. Защита определяет все зашифрованные сообщения и действия, которые должны к ним применяться.

Безопасность электронной почты

Встроенные модули антивирусной проверки и защиты от спама обеспечивают наиболее продвинутой защите от современных интернет-угроз и угроз нулевого дня.

Высокодоступный облачный сервис, размещенный во множестве дата-центров по всему миру, гарантирует повышенную надежность и расширяемость.

UserGate Mail Security способен обеспечить защиту от фишинга, как обычного так и целевого, направленных атак и вирусов. Также продукт сканирует все ссылки в сообщении, чтобы затем проверить источник на наличие вредоносного ПО. Запатентованная технология поиска спама в почтовом трафике RPD (Recurrent-Pattern Detection) обеспечивает уровень детекции спама около 99% и крайне низкий уровень ложного срабатывания - менее, чем одно на 1,5 миллиона сообщений.

Архивирование сообщений

UserGate Mail Security позволяет эффективно организовать корпоративную переписку за счет архивации сообщений. Также продукт предотвращает потерю данных и обеспечивает соответствие требованиям законодательства.

- ✓ Антиспам для любого почтового сервера
- ✓ Защита от потери данных (DLP)
- ✓ Архивирование сообщений
- ✓ Безопасность электронной почты

О продукте

UserGate Mail Security для Exchange Server/SMTP/Lotus – это решение для защиты корпоративной почты от вирусов, фишинга, спама и прочих вредоносных сообщений, позволяющее также предотвращать утечки конфиденциальной информации.

Продукт обеспечивает архивацию сообщений, предоставляет возможность мониторинга почты, поддерживает синхронизацию по IMAP с MS Exchange 2003 и Lotus Domino, а также может работать с любыми другими почтовыми серверами.

Благодаря модульной структуре UserGate Mail Security обладает крайне высокой производительностью и отказоустойчивостью. Облачные модули фильтрации вирусов и спама, обеспечивают фильтрацию спама и защиту от вирусов с крайне быстрым временем реакции на новые угрозы и практически нулевым ложным срабатыванием.

Среднестатистический сотрудник организации со штатом до 1000 человек отправляет и получает 124 электронных письма в течение обычного рабочего дня. Работники крупных компаний отправляют и получают 149 электронных сообщений ежедневно.

Так как 58% содержимого электронных ящиков имеют решающее значение для их успешной работы, а другие коммуникационные средства получают все большее распространение, атаки, направленные через данные каналы связи, представляют угрозу для самой возможности общения и защиты персональных данных частных лиц и компаний.*

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

Защита от утечек персональных данных и иной конфиденциальной информации

Участившиеся случаи «ухода» инсайдерской информации за «стены» компании заставляют представителей руководства различных организаций задумываться о способах устранения данной проблемы. UserGate Mail Security является решением, позволяющим обеспечить конфиденциальность информации, передаваемой с помощью электронной почты.

В системе защиты данных используется три типа фильтрации: регулярные выражения (Regex), сравнение документов (Docmatch) и лемматизатор (Lemmatizer). Каждый из подмодулей, используя разные способы поиска информации в теле, теме, вложениях и других частях письма, исследует почтовые сообщения на наличие в них определенных ключевых слов или фраз и проводит сравнение передаваемых данных с образцами конфиденциальной информации.

Защита от фишинга и вирусов

В UserGate Mail Security интегрированы антивирусные движки Лаборатории Касперского и Panda Security. Данные модули сканируют на наличие угроз весь веб- и FTP-трафик, вложения в электронной почте и скачивания из интернета.

Раннее обнаружение вирусов

Современные вирусы, черви и трояны используют различные слабости антивирусных технологий: основной проблемой является время, необходимое для создания сигнатур или эвристики.

Entensys сотрудничает с международными компаниями, профессионально занимающимися анализом атак и эпидемий. Использование сотен серверов (honeypots) по всему миру позволяет распознавать как спам, так и вирусы, в первую очередь ориентируясь на статистический анализ.

Такой подход обеспечивает самое быстрое время реакции на возникновение новых угроз, что позволяет начинать борьбу с новым вирусом до того момента, как он поразит миллионы компьютеров.

Облачный антиспам

Облачный антиспам отфильтровывает письма, основываясь на анализе их содержания и эвристике. Анализу подвергаются письма на любых языках, а также графические сообщения. Центр обнаружения спама выявляет спамские атаки в любой точке мира.

Одним из важных достоинств облачного антиспама является крайне низкий уровень ложного срабатывания - менее, чем одно на 1,5 миллиона сообщений. При этом уровень детекции составляет более 97%. Традиционный метод блокировки спама на основе черных списков IP и DNS обладает несравненно более высоким уровнем ложного срабатывания. Объяснить это можно тем, что в черные списки часто попадают нормальные пользователи. Достаточно того, чтобы какой-либо компьютер из локальной сети был скомпрометирован и использовался для рассылки спама.

Модуль Entensys Cloud Antispam отправляет облачному сервису UID письма, который определяет, является ли почтовое сообщение спамом. Решение блокирует не IP-адрес, домен или электронный адрес, а конкретное письмо или атаку спама. Таким образом, облачный антиспам может использоваться в организациях, в которых ошибочное удаление писем может приводить к потере клиентов или другим проблемам.

Архивирование сообщений

Копирование входящих сообщений выполняется до антиспам и антивирусной фильтрации. В настройках архивирования можно выбрать направление (только входящие, только исходящие или оба), а также указать адреса исключений.

Интеграция с IMAP

В решении от Entensys реализована интеграция с IMAP-сервером MS Exchange или Lotus Domino. Интеграция предоставляет возможность создания общей папки IMAP на удаленном почтовом сервере и обработку сообщений в этих папках.

Мониторинг и статистика

UserGate Mail Security предоставляет информацию обо всех сообщениях, обработанных сервером решения. Мониторинг сообщений в UserGate Mail Security позволяет выполнять фильтрацию по дате, по статусу обработки (доставлено/заблокировано), по адресу источника или назначения, выполнять принудительную отправку сообщений, заблокированных как спам, а также создавать списки исключений.

Дополнительные методы защиты от спама

Для обработки входящих сообщений в UserGate Mail Server фильтрация выполняется в несколько этапов - по соединениям, по адресу источника, по адресу назначения и по содержанию. UserGate Mail Server поддерживает следующие методы фильтрации спама:

- на основе DNS (DNSBL, RHSBL, Backscatter, MX, SPF, SURBL);
- на основе распределенной антиспам системы (облачный антиспам);
- на основе статистики (собственная реализация фильтрации Байеса).

Кроме этого решение поддерживает контроль SMTP-протокола (контроль правильности команд в соответствии с RFC), ограничивает максимальный размер письма, максимальное количество получателей и т.п.