

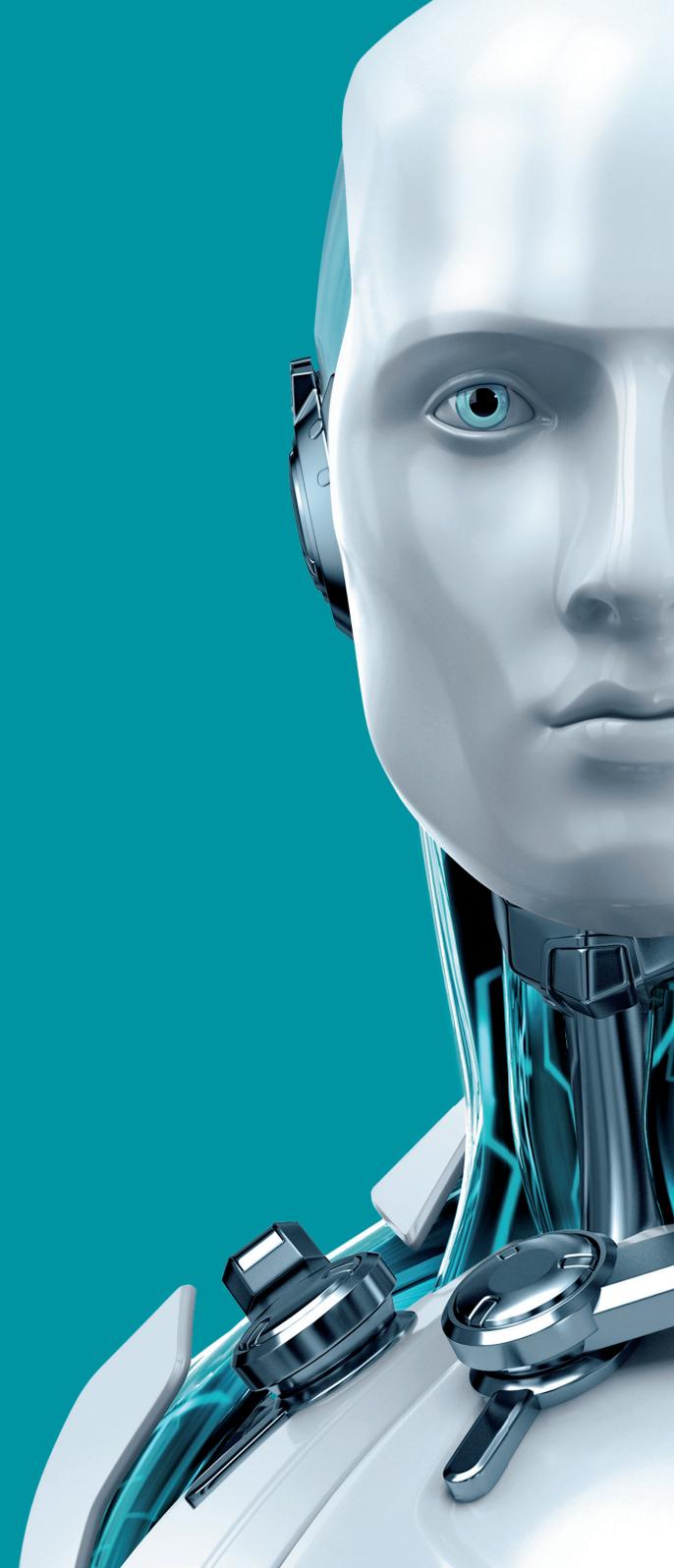


MAIL SECURITY

ДЛЯ MICROSOFT
EXCHANGE SERVER



 АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА





MAIL SECURITY

для MICROSOFT EXCHANGE SERVER

ESET Mail Security для Microsoft Exchange Server предназначен для защиты почтовых серверов от всех типов вредоносного программного обеспечения и для фильтрации почтовых сообщений в режиме реального времени.

Вы получаете полноценную защиту почтового сервера, в том числе защиту его файловой системы. ESET Mail Security для Microsoft Exchange Server позволяет применять политики в отношении конкретного контента на основе реального типа файла, а также отслеживать статус безопасности и легко менять параметры при помощи удобной веб-консоли ESET Remote Administrator.

Антивирусная защита и Антиспам

Антивирус и Антишпион	Устраняют все типы вредоносного программного обеспечения, в том числе вирусы, руткиты, черви и шпионские программы, а также проверяют репутацию приложений до запуска на базе облачной технологии. Для более эффективного обнаружения вредоносных программ и быстрого сканирования облачные технологии ESET проверяют репутацию файлов и добавляют безопасные в «белый» список. В облако отправляется информация только об исполняемых файлах и архивах, которые не содержат личные данные.
Антиспам и Антифишинг	Автоматически блокируют спам и фишинговые рассылки сразу после установки без осуществления дополнительных настроек с высоким процентом определения.
Локальный карантин	Позволяет системным администраторам просматривать подозрительные сообщения через веб-интерфейс и централизованно принимать меры. Системный администратор может разрешить пользователю самому просматривать уведомления о помещении сообщения в карантин и производить действия для одного сообщения или группы. Возможные действия зависят от причины, по которой сообщение было помещено в карантин.
Сканирование базы данных по требованию	Помогает снизить потребление ресурсов системы, выбирая для сканирования только нужные базы данных или отдельные почтовые ящики.
Правила для сообщений	Расширенные настройки фильтрации почтовых сообщений позволяют определить действия для каждого подозрительного сообщения. Параметры фильтрации включают стандартные поля (тема, отправитель, тело сообщения и заголовки). Поврежденные или защищенные паролем архивы и вложения проходят детальную проверку для определения реального типа файла, а не только расширения архива.
Защита от эксплойтов	Устраняет вредоносное ПО, использующее уязвимости в самых распространенных программных продуктах, включая веб-браузеры, PDF-редакторы, почтовые клиенты, Microsoft Office и Java. Кроме того, блокировщик эксплойтов контролирует поведение процессов и выявляет подозрительную активность, которая является типичной для целевых атак и атак нулевого дня.
Расширенное сканирование памяти	Технология позволяет обезвреживать зашифрованные вредоносные программы, которые устанавливаются на компьютер скрыто от пользователя.
HIPS	Система предотвращения вторжений защищает от вредоносных программ и другой нежелательной активности, которая может негативно повлиять на безопасность компьютера. Расширенный анализ поведения в сочетании с возможностями сетевой фильтрации по обнаружению позволяет отслеживать запущенные процессы, файлы и разделы реестра.
Контроль устройств	Автоматическое сканирование подключаемых внешних устройств и настройка правил работы со съемными носителями информации для каждого пользователя. Блокирует несанкционированное подключение устройств к серверу. Позволяет создавать правила для групп пользователей, соответствующие политикам безопасности компании. Тактично уведомляет пользователя о том, что подключенное устройство заблокировано, и дает дальнейшие инструкции для Microsoft Exchange Server

Специализированные функции

Независимость от снимков системы	Возможность указать альтернативные пути для хранения файлов обновления при начальной установке, что позволяет восстановить актуальную версию продукта при откате системы без повторного скачивания большого объема данных.
Поддержка кластерной структуры	Возможность соединить несколько продуктов, установленных в кластере, в единое решение для централизованного управления. Позволяет настроить решение для автоматического дублирования параметров при установке в кластерной среде и управлять им как единым целым, устраняя необходимость ручного дублирования изменений для других узлов в кластере.
ESET Shared Local Cache	Сохраняет метаданные о «чистых» файлах с ранее проверенных машин в рамках одного гипервизора. Благодаря этому проверенные на одной виртуальной машине файлы не сканируются повторно на других машинах в рамках одной виртуальной среды. Такой подход позволяет существенно снизить общую нагрузку при проверке виртуальных машин.
Поддержка Windows Management Instrumentation	Управление ESET Mail Security для Microsoft Exchange Server при помощи WMI позволяет интегрировать продукт в другие решения для мониторинга сети и продукты класса SIEM (Security Information and Event Management).



БЕСПЛАТНАЯ
ТЕХНИЧЕСКАЯ
ПОДДЕРЖКА

Экономьте свое время благодаря нашим специалистам.

Режим работы технической поддержки: круглосуточно, ежедневно, на русском языке.

Дополнительные возможности:

Исключения для процессов	Администратор может исключить определенные процессы из сканирования в режиме реального времени – все файловые операции, которые могут быть связаны с этими процессами, будут априори считаться безопасными. Особенно это важно для случаев, когда определенные процессы, такие как резервное копирование или миграция виртуальной машины без ее выключения, мешают работе защиты в режиме реального времени. Данная возможность повышает совместимость с программным обеспечением сторонних производителей.
Легкие и быстрые пакеты обновлений	Небольшие пакеты обновлений в сочетании с облачными технологиями обнаружения угроз обеспечивают быстрое и точное сканирование вредоносных объектов.
Модульная установка	При установке продукта можно выбрать необходимые компоненты: <ul style="list-style-type: none">- защита файловой системы в режиме реального времени;- защита почты и интернета;- контроль устройств;- графический интерфейс;- ESET Log Collector и др.
Централизованное управление	Продуктом ESET Mail Security для Microsoft Exchange Server можно удаленно управлять при помощи ESET Remote Administrator. Развернуть решение, запустить задачи, установить политики безопасности, формировать журналы, получать уведомления и обзор безопасности всей сети можно с единой веб-консоли.
ESET Log Collector	Простая утилита, которая служит для упрощения сбора файлов журналов антивируса ESET, файлов конфигурации ПО ESET, журналов системных ошибок, информации о запущенных на компьютере пользователя процессах. Вся информация собирается в один архив, который можно отправить по почте или загрузить на общий сетевой диск для ускорения устранения неполадок.
ESET License Administrator	Интернет-портал, где владелец лицензии на продукты ESET может управлять всеми лицензиями, видеть, где они используются, а также делегировать часть прав администраторам безопасности.

Copyright © 1992—2018 ESET, spol. s r. o., логотипы ESET, NOD32, ThreatSense и другие упомянутые продукты зарегистрированы под торговой маркой ESET, spol. s r. o. Другие упомянутые компании, логотипы, изображения или продукты могут быть зарегистрированными торговыми марками их владельцев. Произведен согласно качественным стандартам ISO 9001:2000.