UserGate Log Analyzer

Виртуальная платформа UserGate Log Analyzer VE

Модели: VE 6 | VE 14 | VE 25

UserGate Log Analyzer Virtual Edition позволяет быстро развернуть виртуальную машину, с уже настроенными компонентами. Образ создан в формате OVF (Open Virtualization Format).

Для организаций, которые предпочитают использовать виртуальную инфраструктуру.

Спецификация	VE 6	VE 14	VE 25
Объем хранилища, Тбайт	6	14	25
Количество пользователей	3 000	5 000	10 000

ОСНОВНЫЕ ФУНКЦИИ

- Уменьшение нагрузки на шлюзы UserGate
- Обработка журналов и создание отчетов
- Объединение журналов с нескольких шлюзов для общего анализа
- Увеличение глубины журналирования
- Увеличение размера хранилища на серверах LogAn
- Сбор и анализ информации со сторонних устройств

Аппаратная платформа UserGate Log Analyzer E6, E14

Модели: E6 | E14

UserGate Log Analyzer E дополняет функциональность серверного решения UserGate и предназначен для агрегации данных, связанных с анализом инцидентов безопасности, а также для осуществления мониторинга событий и создания отчетов.

Для крупных банков и заводов, администраций, ведомственных подразделений, университетов.

Спецификация	E 6	E 14
Объем хранилища, Тбайт	6	14
Количество пользователей	3 000	5 000

Аппаратная платформа UserGate Log Analyzer F25

Модели: F25

UserGate Log Analyzer F25 предназначен для использования в крупных компаниях и дата-центрах. Данный программно-аппаратный комплекс обладает большими возможностями по хранению информации и обеспечивает максимально быструю обработку данных, получаемых от серверов UserGate.

Для крупных корпоративных сетей, ритейла, дата-центров, университетов, министерств.

Спецификация	F 25
Объем хранилища, Тбайт	25
Количество пользователей	10 000

Анализ инцидентов ИБ

Система анализа событий и инцидентов UserGate Log Analyzer

UserGate Log Analyzer является комплексным решением для анализа данных. Система агрегирует данные от различных устройств, осуществляет мониторинг событий и создает отчеты. Появление новых угроз и увеличение объема обрабатываемой информации предъявляет повышенные требования к скорости работы системы анализа.

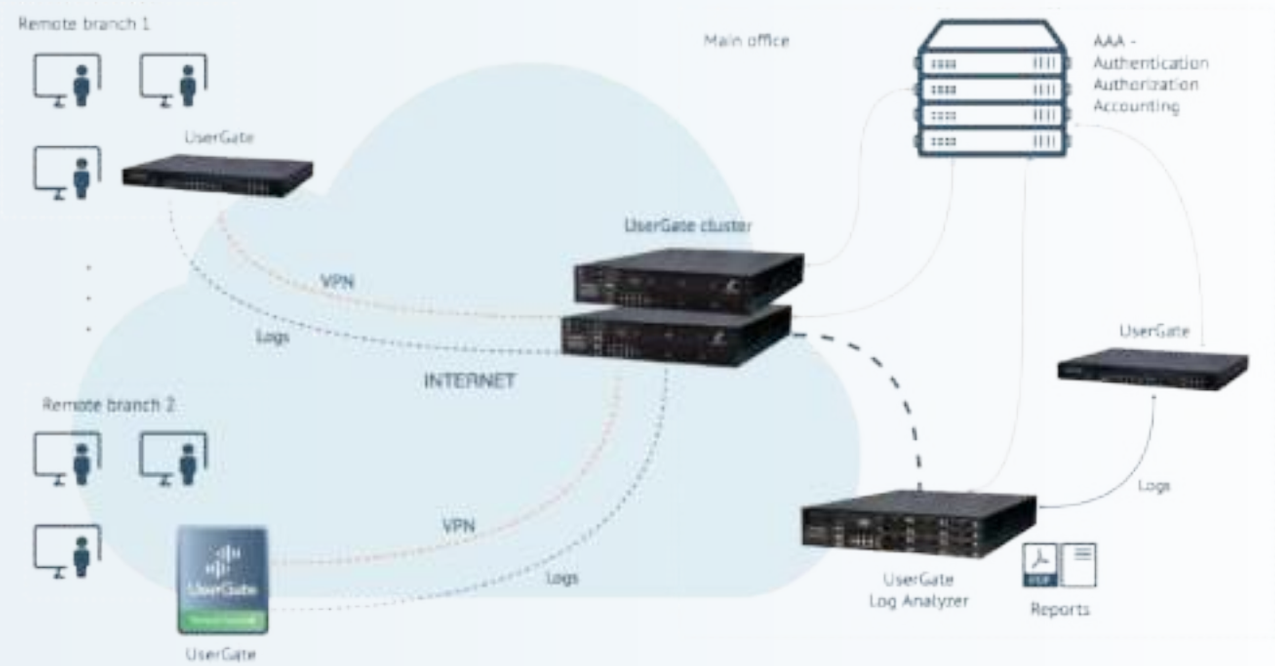
Решение UserGate Log Analyzer развертывается отдельно от шлюза безопасности. Разделение функций обработки трафика и анализа данных позволяет обеспечить высокую надежность и хорошую масштабируемость системы. Получаемые и обрабатываемые данные можно агрегировать с нескольких серверов. Использование отдельного сервера для анализа журналов снижает нагрузку на межсетевые экраны и позволяет обрабатывать больший объем данных.

Основные возможности

UserGate Log Analyzer осуществляет сбор и первичную обработку данных от межсетевых экранов NGFW UserGate. На основании полученных данных осуществляется глубокий анализ произошедших событий безопасности, определяются и отслеживаются подозрительные активности отдельных пользователей или хостов, что в том числе необходимо для соответствия современной концепции SOAR (Security Automation, Orchestration and Response).

При настройке UserGate администратор может указать, какие типы событий пересылаются для анализа в Log Analyzer. Опции для выбора включают журнал событий, журнал системы обнаружения вторжений, журналы трафика, событий АСУ ТП, а также события из журнала веб-доступа.

В секции подготовки отчетов располагаются готовые шаблоны отчетов и правила их обработки. В этой же секции доступны выполненные по запросу администратора отчеты.



Контактная информация

Телефон: **8 (800) 500 4032**
Клиентам: **sales@usergate.ru**
Партнерам: **partner@usergate.ru**

121205, г. Москва, ул. Нобеля, 7, этаж 4
630090, г. Новосибирск, ул. Николаева, 11, офис 602
680021, г. Хабаровск, ул. Ленинградская, 46, офис 2