

UserGate Log Analyzer



Появление новых угроз информационной безопасности и увеличение объема обрабатываемой информации предъявляет повышенные требования к скорости и качеству работы систем анализа. Для решения этой задачи UserGate предлагает комплексное решение для анализа данных – UserGate Log Analyzer (LogAn).

UserGate Log Analyzer

- агрегирует данные от различных устройств
- осуществляет мониторинг событий
- создает отчеты
- обеспечивает долгосрочное хранение логов
- снижает нагрузку на межсетевые экраны

UserGate Log Analyzer

разворачивается на операционной системе UGOS¹ и использует технологию User ID².

UserGate Log Analyzer

внесен в Единый реестр российского ПО № 6919 от 01.09.2020 года.

¹ UGOS

При разработке собственной операционной системы UGOS компания UserGate отказалась от использования open-source-модели и сосредоточилась на создании проприетарного кода.

Такой подход позволяет решениям UserGate обрабатывать и анализировать сетевой трафик на высоконагруженных каналах связи, добиваться эффективного масштабирования и обеспечивать подлинную безопасность информационной инфраструктуры своих заказчиков.

² User ID

UserID — технология прозрачной аутентификации пользователей на устройствах UserGate Log Analyzer и UserGate NGFW.



Принцип работы UserGate Log Analyzer

UserGate Log Analyzer осуществляет сбор и первичную обработку данных от межсетевых экранов следующего поколения UserGate NGFW.

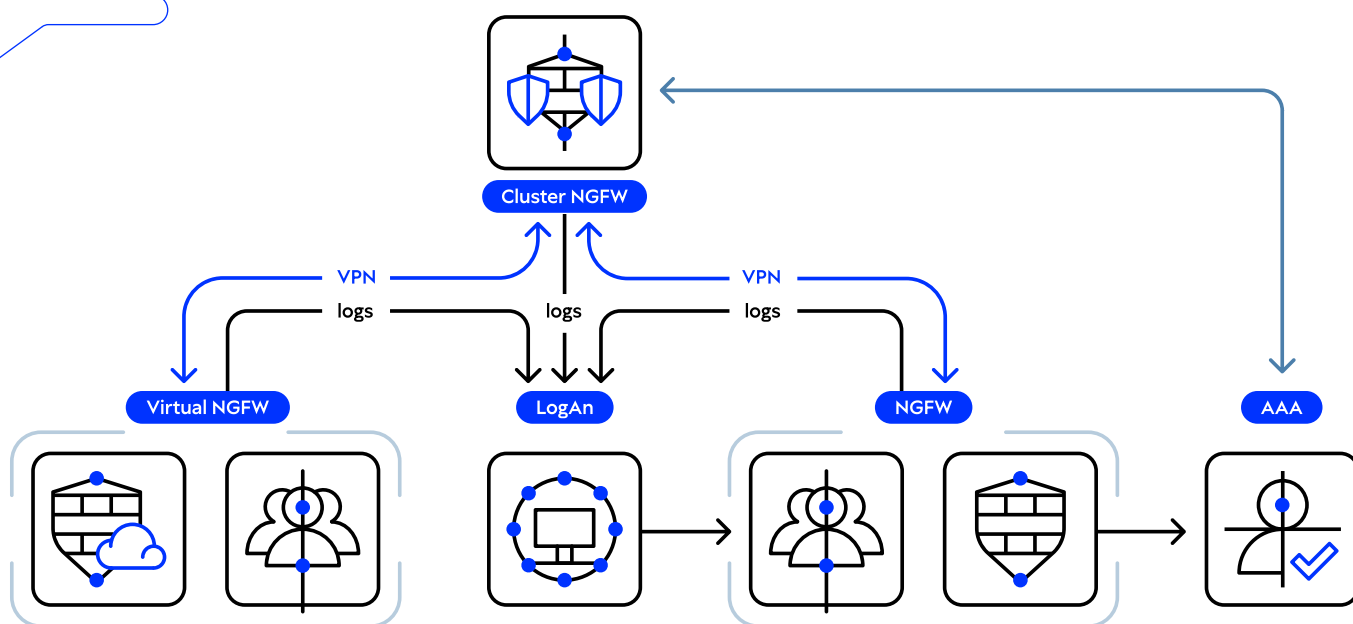
При настройке UserGate NGFW администратор может выбрать, какие типы событий отправлять для анализа в UserGate Log Analyzer.

Типы и источники событий для выбора:

- журнал событий
- журнал системы обнаружения вторжений (СОВ)
- журнал трафика
- журнал событий АСУ ТП
- журнал веб-доступа

UserGate Log Analyzer на основании полученных данных:

- осуществляет глубокий анализ произошедших событий безопасности
- определяет и отслеживает подозрительные активности пользователей или хостов



Функции UserGate Log Analyzer

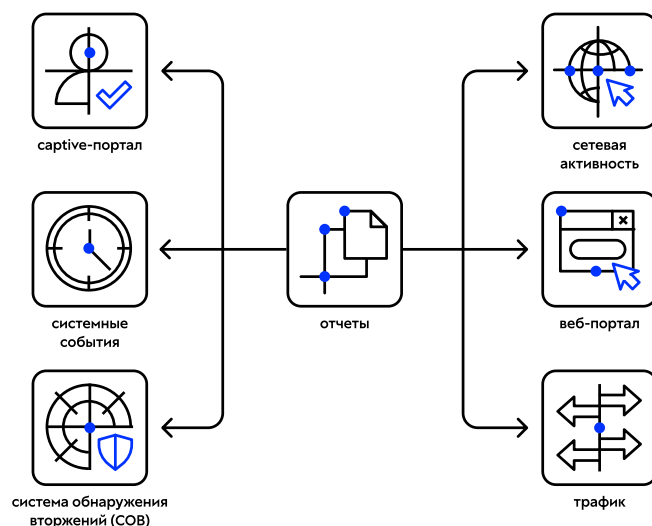
- **Сбор информации**
Агрегация событий из различных источников в единой базе позволяет удобно работать с ними.
- **Нормализация информации**
Приведение событий к единому формату облегчает поиск необходимых логов, анализ и сравнение данных.
- **Долгосрочное хранение информации**
Возможность обращаться к историческим событиям помогает в расследовании инцидентов.
- **Отчетность**
Дашборды, виджеты и отчеты качественно оптимизируют работу с большим количеством данных.

Сценарии использования отчетов UserGate Log Analyzer

Во вкладке «Отчеты» интерфейса UserGate Log Analyzer располагаются готовые шаблоны и правила их обработки. Здесь же хранятся отчеты, выполненные ранее по запросу администратора.

Категории отчетов

- **Captive-портал**
группа шаблонов по событиям, авторизации пользователей с помощью Captive-портала.
- **Системные события**
отчеты по событиям включают информацию об авторизации через консоль, сводные отчеты о действиях администраторов, изменениях конфигураций по компонентам и системных событиях по степени критичности.
- **Система обнаружения вторжений (СОВ)**
отчеты категории СОВ предоставляют детальную информацию об атаках: определяется топ IP-адресов источников атак, цели атакующих (IP-адреса хостов), топ протоколов, используемых в атаках. Также из отчета можно получить информацию по используемым устройствам и топ сигнатур устройств. При наличии captive-портала доступна информация об авторизациях через captive-portal по времени суток, дню недели, дню месяца и суммарная информация за месяц.
- **Сетевая активность**
отслеживание сетевой активности с помощью анализа DoS-событий по времени суток, дням месяца, неделям и месяцам. Доступна информация по заблокированным приложениям, пользователям, наибольшему количеству заблокированных приложений и сработавших правил.
- **Веб-портал**
группа шаблонов авторизации через SSL VPN.
- **Трафик**
детальная информация по трафику пользователей за день, неделю, месяц, а также наибольшему количеству приложений по пользователям, странам, источнику и назначению трафика.
- **Веб-активность**
список всех посещенных веб-сайтов, блокируемых доменов и пользователей по URL-категориям и заблокированным сайтам.



Автоматическое уведомление

Сформированные отчеты автоматически высылаются по электронной почте администратору и другим уполномоченным сотрудникам. Расписание отправки отчетов можно настроить, указав время и день недели.

Выявление потенциальных угроз

Использование отчетов из различных категорий позволяет выявить потенциальные угрозы на основе анализа произошедших событий.

Соответствие требованиям корпоративной политики безопасности

UserGate Log Analyzer позволяет сопоставить результаты отчетов с установленными параметрами сети и обеспечить соответствие инфраструктуры требованиям корпоративной политики безопасности.

Преимущества UserGate Log Analyzer

Надежность и масштабируемость

- UserGate Log Analyzer разворачивается отдельно от шлюза безопасности.
- Разделение функций обработки трафика и анализа данных позволяет обеспечить высокую надежность и масштабируемость системы.
- Получение, обработка и агрегирование данных производится с нескольких серверов.
- Использование отдельного сервера для анализа журналов снижает нагрузку на межсетевые экраны и позволяет обрабатывать большой объем данных.

Простота настройки и эксплуатации

- Самостоятельная установка системы занимает не более 15 минут.
- Простота настройки, удобный поиск событий и хранение логов позволяют существенно оптимизировать ресурсы внутренней ИБ-команды.

Кластерная архитектура

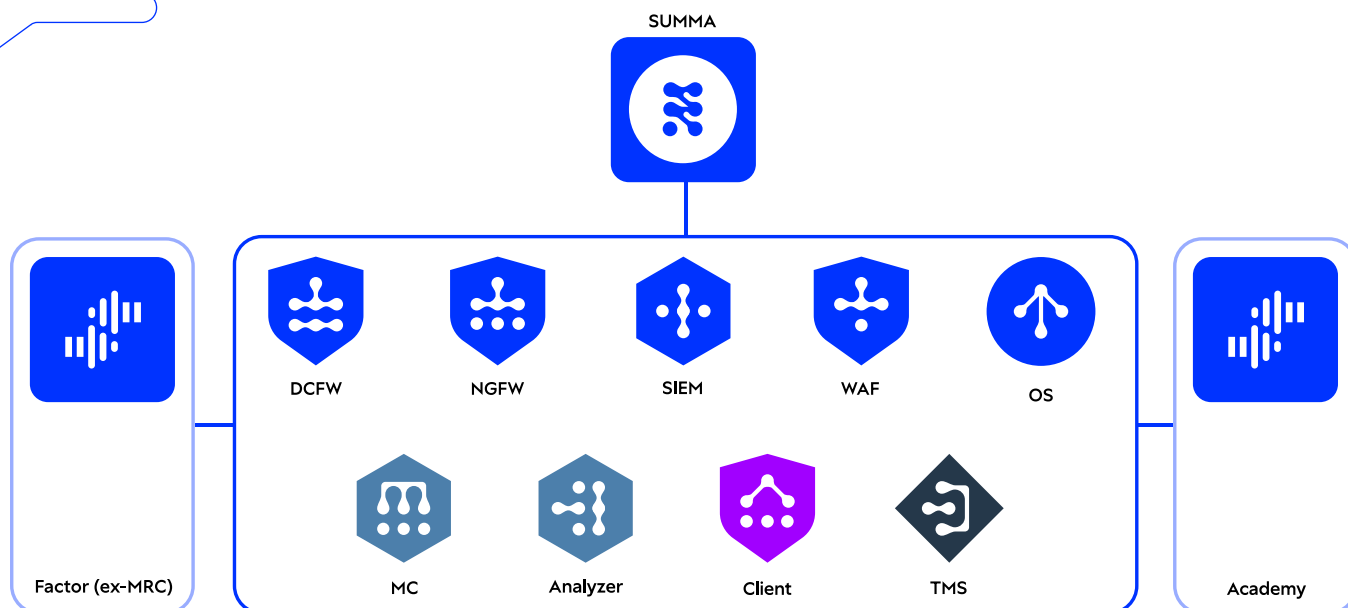
- Автоматический переход нагрузки между узлами кластера при сбоях минимизирует простои системы.
- Узлы обновляются последовательно без остановки, позволяя системе работать в режиме 24/7.
- Резервирование информации предотвращает потерю данных.

Соответствие требованиям законодательства РФ

- UserGate Log Analyzer внесен в Единый реестр российского ПО № 6919 от 01.09.2020 года.

Интеграция с продуктами экосистемы безопасности UserGate SUMMA

- Максимальная скорость взаимодействия достигается с межсетевыми экранами следующего поколения UserGate NGFW.
- Использование UserGate Log Analyzer в сочетании с продуктами UserGate SUMMA создает условия для максимальной видимости событий и закрывает потребности организации в надежной защите.



Формы поставки UserGate Log Analyzer

Модельный ряд и технические характеристики

Аппаратная платформа UserGate Log Analyzer E6, E14, F25

	Log Analyzer E6	Log Analyzer E14	Log Analyzer F25
Объем хранилища, Тбайт	6	14	25
Количество ядер	8	8	32
Память, Гбайт	32	32	64
Применение	Филиалы, малые офисы, промышленные объекты	Предприятия, госсектор, учреждения образования	ЦОД, крупные сети

Виртуальные платформы UserGate Log Analyzer VE6, VE14, VE25

	VE6	VE14	VE25
Объем хранилища, Тбайт	6	14	25
Количество ядер	6	12	32
Память, Гбайт	32	32	64
Применение	Филиалы, малые офисы, промышленные объекты	Предприятия, госсектор, учреждения образования	ЦОД, крупные сети

Поддержка всех популярных средств виртуализации:



Облачное исполнение

Поддержка любых облаков, работающих по стандартам реализации VMware и KVM (OpenStack).

Отправить запрос



Контактная информация:

Телефон: 8 (800) 500-40-32
Клиентам: sales@usergate.ru
Партнерам: partner@usergate.ru
Маркетинг: marketing@usergate.ru

© 2025 ООО «Юзергейт»
Все права защищены

Полезные ресурсы UserGate:

usergate.com/ru
t.me/usergatenews
rutube.ru/channel/24630896/
vk.com/usergaterus

