

UserGate Log Analyzer

АНАЛИЗ ДАННЫХ И РЕАКЦИЯ НА УГРОЗЫ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



UserGate SUMMA

СЛАГАЕМЫЕ БЕЗОПАСНОСТИ

Экосистема решений для комплексного подхода к обеспечению информационной безопасности

АНАЛИЗ СОБЫТИЙ И ИНЦИДЕНТОВ ОТ USERGATE

UserGate Log Analyzer

Современный ландшафт угроз настолько разнообразен и динамичен, что использование базовых средств обеспечения безопасности уже не является достаточным для построения защищенной инфраструктуры.

Для обеспечения информационной безопасности предприятий и организаций необходимо анализировать данные, находить среди них значимые события безопасности, выявлять инциденты и расследовать их.

Функции UserGate Log Analyzer

SIEM&IRP

UserGate Log Analyzer (LogAn) сочетает в себе функции SIEM (Security Information and Event Management – управление событиями и инцидентами о безопасности) и IRP (Incident Response Platform – реагирование на инциденты безопасности). Это предоставляет пользователям возможности сбора логов и событий, поиска инцидентов и реагирования на них.

SOAR

Удобная система оркестрирования, автоматизации и реагирования на события безопасности позволяет реализовать концепцию SOAR (Security Orchestration, Automation and Response – оркестрирование, автоматизация и управление системами безопасности) в рамках экосистемы UserGate SUMMA.

Возможности и преимущества UserGate Log Analyzer

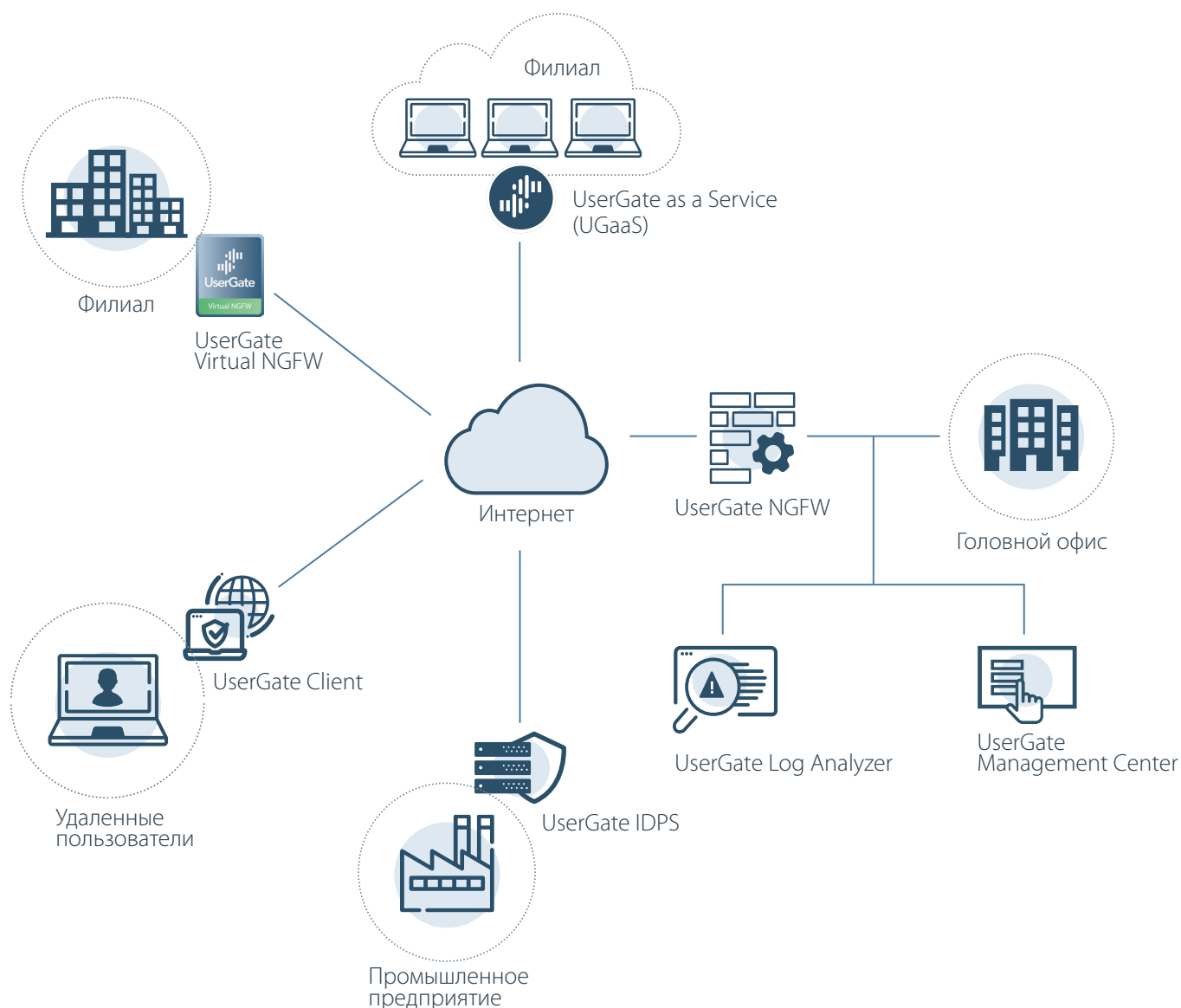
- оценка состояния информационной безопасности компании;
- мониторинг событий безопасности в реальном времени и расследование инцидентов;
- ретроспективный анализ событий безопасности, хранение и резервирование данных;
- сокращение времени реакции на инцидент;
- обеспечение непрерывности бизнес-процессов;
- видимость событий безопасности;
- доступность данных корпоративного уровня;
- автоматизация процессов безопасности;
- подключение к личному кабинету ГосСОПКА и отправка информации об инцидентах в ручном или в автоматическом режимах.

Соответствие требованиям законодательства РФ:

Сертификат ФСТЭК России № 3905.

Как действует экосистема безопасности UserGate SUMMA

- UserGate LogAn собирает данные со всех продуктов экосистемы безопасности UserGate SUMMA и сторонних устройств.
- UserGate LogAn позволяет обогащать данные для поиска IoC (индикаторов компрометации), а также создавать свои IoC в результате расследования инцидентов. Эти данные (IP-адреса, URL-адреса, hash файла и т. д.) могут быть использованы в экосистеме UserGate SUMMA для блокировки вредоносной активности и предотвращения повторения инцидентов.
- UserGate LogAn отправляет уведомления в UserGate Management Center, который, в свою очередь, посылает управляющие команды в UserGate NGFW и UserGate Client для оперативного реагирования на события безопасности (SOAR).



ЛИНЕЙКА USERGATE LOG ANALYZER

Защита информационной инфраструктуры в виртуальной среде



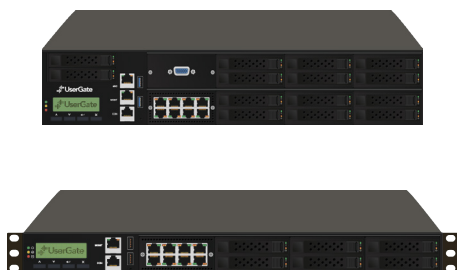
Виртуальная платформа UserGate Log Analyzer VE

Модели: VE 6 | VE 14 | VE 25

Альтернатива аппаратным решениям.
Быстрое развертывание и масштабирование.

Спецификация	VE6	VE14	VE25
Объем хранилища, Тбайт	6	14	25
Количество ядер	6	12	32
Память, Гбайт	32	32	64

Защита информационной инфраструктуры средних и крупных организаций



Аппаратные платформы UserGate Log Analyzer

Модели: E6 | E14 | F25

Расширение функций серверного решения UserGate.
Хранение и обработка массивов данных, получаемых от серверов UserGate.

Спецификация	E6	E14	F25
Объем хранилища, Тбайт	6	14	25
Количество ядер	8	8	32
Память, Гбайт	32	32	64

Продукты экосистемы UserGate SUMMA

UserGate NGFW ●

Межсетевой экран нового поколения UserGate предоставляет функции безопасности для сетей любого формата и размера, обеспечивая максимальную видимость событий и высокий уровень защиты от угроз. Огромную роль в построении защищенной инфраструктуры играет возможность увидеть, проанализировать и интерпретировать все события безопасности, к которым относятся действия пользователей, приложений и устройств. Для этого необходимо обеспечивать качественную и производительную инспекцию SSL-трафика. Благодаря передовым технологиям UserGate межсетевой экран нового поколения может дешифровать весь трафик, включая TLS 1.3 и TLS GOST.

UserGate Management Center ●

Централизованная система управления экосистемой безопасности UserGate SUMMA корпоративного уровня. С помощью UGMC настраиваются все параметры работы межсетевых экранов UserGate: сетевые настройки, правила межсетевого экранирования, контентной фильтрации, системы обнаружения вторжений и другие. UGMC позволяет систематизировать подход к составлению настроек через применение шаблонов, а также прозрачно применить эти настройки на выбранной части парка межсетевых экранов. Среди основных функций UGMC: централизованное управление, автоматизация безопасности, ролевой доступ администраторов, контроль обновлений.

Модуль IDPS UserGate ●

Для обнаружения вредоносной активности предприятиям необходимо проводить непрерывный мониторинг трафика. В этом помогают средства обнаружения и предотвращения вторжений (COB или IDPS). В составе UserGate NGFW присутствует собственный высокопроизводительный модуль COB/IDPS. Администратор может создавать различные наборы сигнатур, релевантных для защиты определенных сервисов, и задавать правила, определяющие действия для выбранного типа трафика, который будет проверяться в соответствии с назначенными профилями.

UserGate Log Analyzer ● (SIEM, IRP, SOAR)

Современный ландшафт угроз настолько разнообразен и динамичен, что не достаточно использовать только базовые средства обеспечения безопасности. UserGate Log Analyzer (LogAn) сочетает в себе функции SIEM (Security Information and Event Management) и IRP (Incident Response Platform), что предоставляет возможности для сбора логов и событий, поиска инцидентов и реагирования на них. Удобная система оркестрирования, автоматизации и реагирования на события безопасности позволяет также реализовать концепцию SOAR (Security Orchestration, Automation and Response) в рамках экосистемы UserGate SUMMA.

UserGate Client ● (EDR, ZTNA, NAC)

Программное обеспечение класса Endpoint Detection & Response (EDR) для конечных устройств. UserGate Client обеспечивает видимость событий безопасности, контроль и сетевой доступ с нулевым доверием (Zero Trust Network Access). Программный продукт централизованно развертывается на тысячах устройств, осуществляет сбор логов, журналов и отчетов для SIEM-системы UserGate Log Analyzer, позволяет быстро и безопасно подключаться к корпоративным сетям по VPN-туннелям, обеспечивает запись и хранение информации о сетевой активности и действиях пользователей в конечных точках.

Модуль WAF UserGate ● (релиз ожидается)

Применение Web Application Firewall считается наиболее эффективным подходом к защите веб-ресурсов. Модуль WAF экосистемы UserGate SUMMA устанавливается на физический или виртуальный сервер и может выявлять разнообразные виды атак. Этот инструмент фильтрации трафика работает на прикладном уровне и защищает веб-приложения методом анализа трафика HTTP/HTTPS и семантики XML/SOAP.



Контактная информация:

Телефон: 8 (800) 500 4032

Клиентам: sales@usergate.ru

Партнерам: partner@usergate.ru

usergate.ru

© 2022 ООО «Юзергейт». Все права защищены.