UserGate

UserGate Client

ЗАЩИТА КОНЕЧНЫХ УСТРОЙСТВ ОТ СОВРЕМЕННЫХ УГРОЗ

Видимость событий безопасности
Контроль
Нулевое доверие

UserGate SUMMA

СЛАГАЕМЫЕ БЕЗОПАСНОСТИ

Экосистема решений для комплексного подхода к обеспечению информационной безопасности

UserGate Client – программное обеспечение класса Endpoint Detection & Response (EDR) для конечных станций.

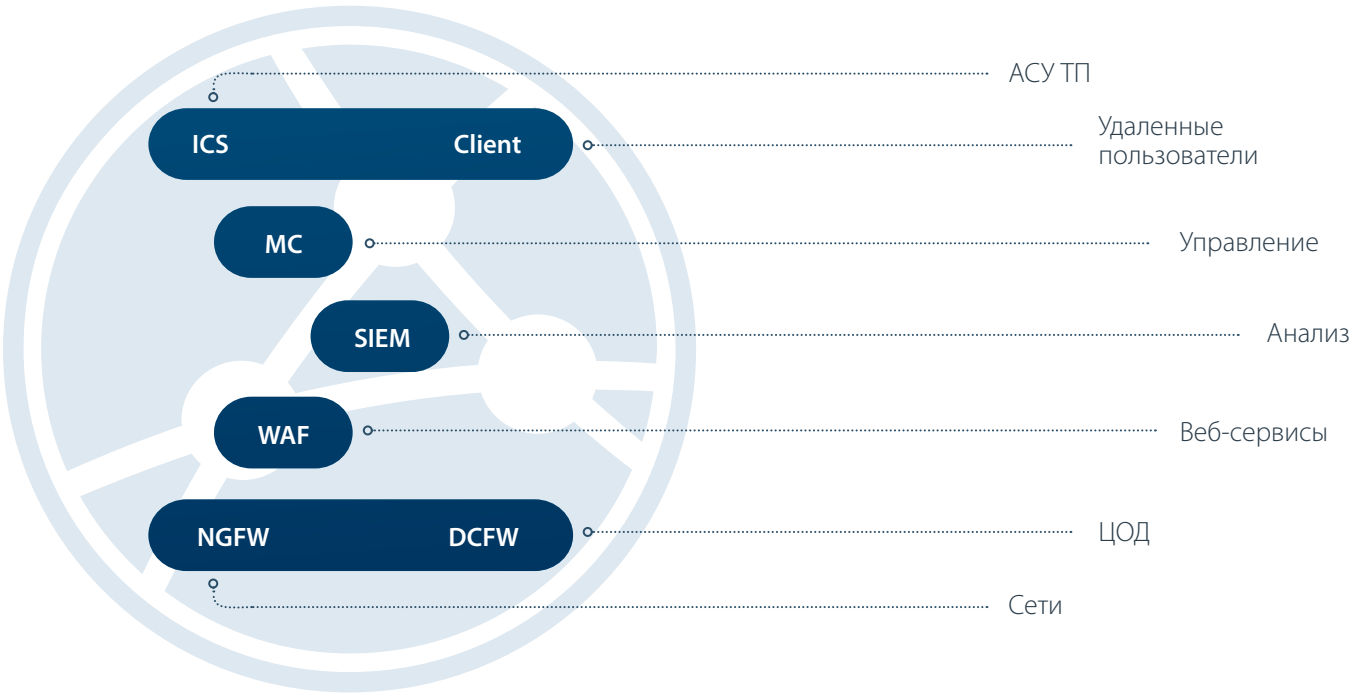
UserGate Client

В условиях массового удаленного доступа и развития интернета вещей каждое устройство в корпоративной сети может стать точкой входа для злоумышленников и вредоносного ПО.

Безопасность конечных станций является важным компонентом современной сетевой безопасности, поскольку все большее количество различных устройств используются для входа в корпоративную сеть для решения ежедневных бизнес-задач.

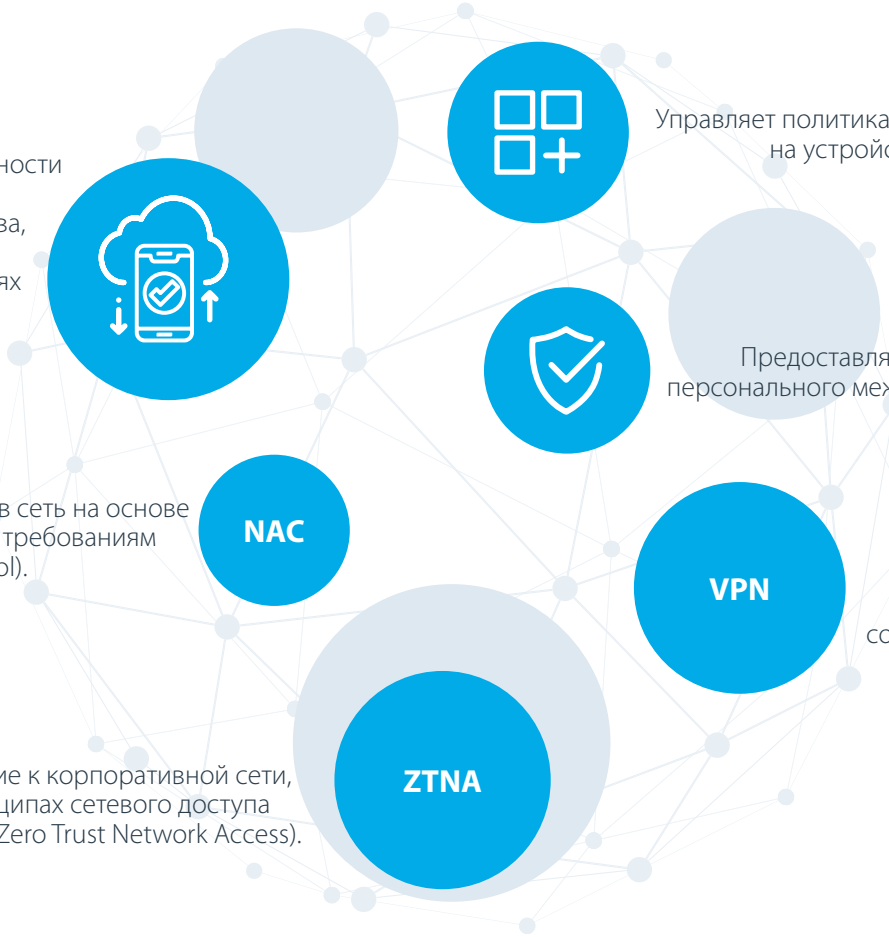
С помощью решений UserGate вы сможете создать интегрированную систему компонентов отслеживания, управления и расширенной защиты конечных точек, входящих в ваше сетевое окружение, и обеспечить надежную защиту своих IT-ресурсов.

UserGate Client – агент UserGate SUMMA. Обеспечивает видимость событий безопасности, контроль и сетевой доступ с нулевым доверием (ZTNA).



Подключаясь к UserGate SUMMA, UserGate Client предоставляет дополнительную информацию о конечной точке и обеспечивает возможность контролировать устройство внутри и за пределами периметра сети.

Функции UserGate Client



Сообщает экосистеме компонентов безопасности UserGate SUMMA о состоянии устройства, работающих на нем приложениях и версиях ПО.

Управляет политиками используемых на устройстве приложений.

Предоставляет защиту уровня персонального межсетевого экрана.

Контролирует доступ в сеть на основе политик соответствия требованиям (Network Access Control).

Обеспечивает безопасное удаленное соединение (Virtual Private Network).

Реализует подключение к корпоративной сети, построенное на принципах сетевого доступа с нулевым доверием (Zero Trust Network Access).

Преимущества UserGate Client

- Является важным компонентом реализации концепции сетевого доступа с нулевым доверием (ZTNA).
- 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 защищенным каналам связи.
- Обеспечивает запись и хранение информации о сетевой активности и действиях пользователей в конечных точках.
- Соответствует требованиям российского законодательства (UserGate Client внесен в реестр российского программного обеспечения, запись в реестре 13087).

Механизмы использования UserGate Client

EDR

Классический EDR (Endpoint Detection & Response)

EDR состоит из агентов UserGate Client, устанавливаемых на конечные точки, и серверной части (UserGate Management Center + UserGate Log Analyzer). UserGate Client ведет мониторинг конечной точки и передает данные о событиях безопасности в UserGate Log Analyzer.

UserGate Log Analyzer анализирует полученные данные, сопоставляет их с базами индикаторов компрометации (IoC) и другой доступной информацией о сложных угрозах. При обнаружении события с признаками киберинцидента EDR-система оповещает сотрудников службы безопасности, а также блокирует сетевую активность, заводит инцидент безопасности и выполняет другие действия благодаря возможностям интеграции в рамках экосистемы UserGate SUMMA.

NAC

Контроль доступа к сети (Network Access Control, NAC)

NAC состоит из агентов UserGate Client, сервера управления UserGate Management Center, сервера аналитики UserGate Log Analyzer и межсетевого экрана UserGate NGFW.

UserGate Management Center формирует правила безопасности для доступа в сеть, основываясь на данных конечного устройства (версия ОС, наличие обновлений, наличие конкретного ПО и т.д.). UserGate NGFW получает информацию о соответствии конечного устройства политикам безопасности и принимает решение о предоставлении доступа.

Защита конечных точек вне периметра

UserGate Client имеет функционал межсетевого экрана уровня узла. Это позволяет сохранить уровень защиты конечного устройства при покидании периметра сети. При любой удаленной работе сохранится возможность фильтровать вредоносные и запрещенные сайты, а также обеспечивать защиту сетевых соединений от различных угроз.

VPN

Подключение к защищенной сети (VPN)

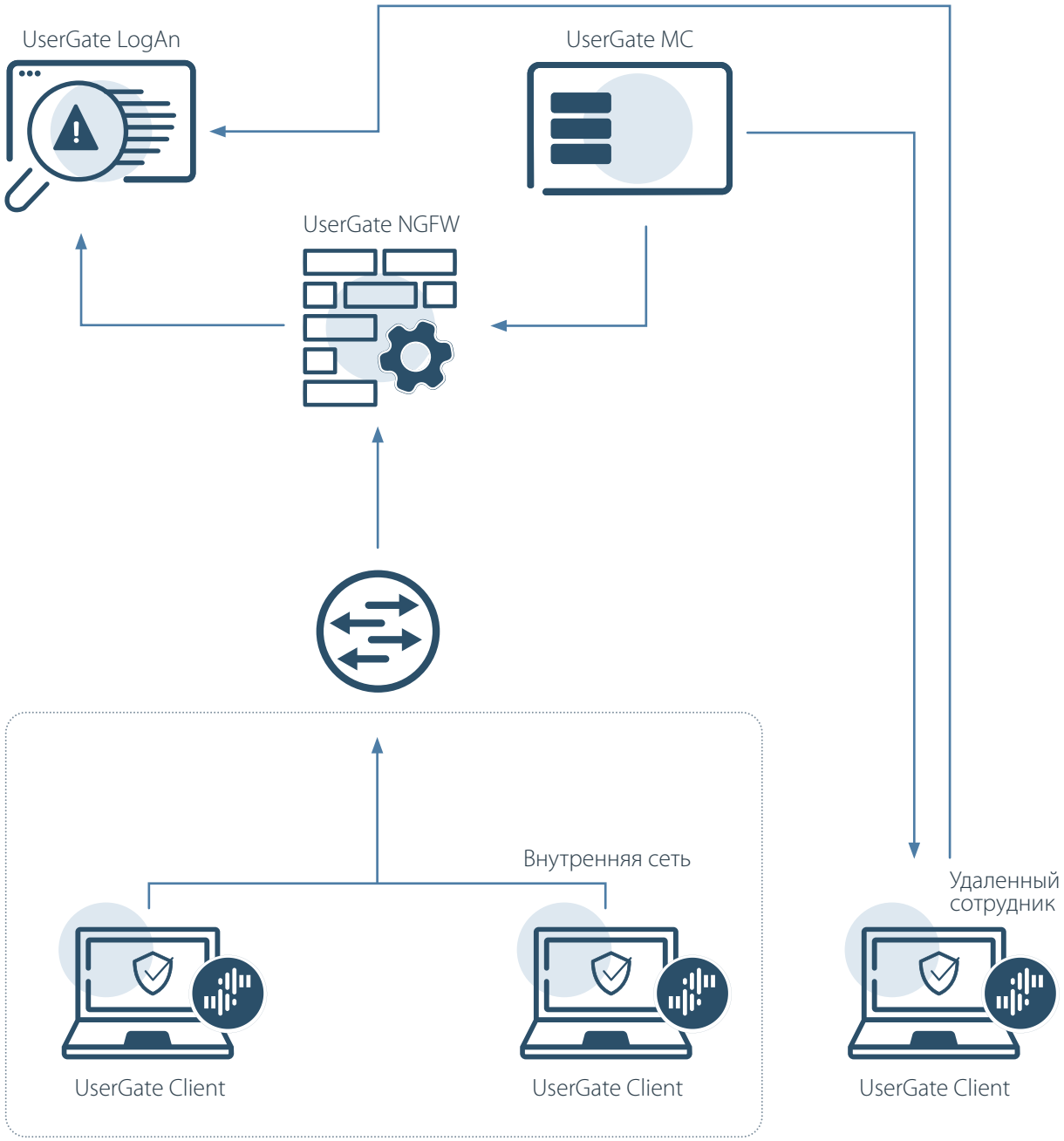
UserGate Client имеет возможность подключаться к защищенным корпоративным сетям посредством встроенного VPN-клиента. Алгоритмы шифрования трафика позволяют безопасно получать доступ к внутренним ресурсам и данным организации вне зависимости от местоположения сотрудника и его устройства. Дополнительные механизмы аутентификации (Multi-Factor Authentication, MFA) позволят предоставить доступ только тем пользователям, которые прошли соответствующую проверку.

ZTNA

Компонент сетей с нулевым доверием (ZTNA)

С помощью UserGate Client появляется возможность организовать архитектуру нулевого доверия (Zero Trust Network Access, ZTNA) в корпоративной сети за счет механизмов аутентификации пользователей и политик допуска устройств в сеть. Дополнительные проверки позволяют снизить риск неправомерного доступа к IT-инфраструктуре, а также гранулярно разграничить приложения, к которым будет предоставлен доступ.

Механизмы использования UserGate Client



Экспертиза UserGate

С помощью пакетов экспертизы от MRC UserGate (Центр мониторинга и реагирования) можно обнаруживать следы компрометации (IoC) на конечных станциях, а также блокировать вредоносную активность в случае обнаружения инцидента.

UserGate Client поставляется в виде:

- программного комплекса как агент экосистемы безопасности UserGate SUMMA, включающего в себя лицензию для централизованного управления через UserGate Management Center и передачи данных в UserGate Log Analyzer;
- по сервисной модели Безопасность как услуга (Security as a Service).

С помощью разных форм поставки перед вами открывается множество сценариев встраивания функций безопасности UserGate в вашу IT-архитектуру.

Требования к установке UserGate Client

Программный продукт UserGate Client может быть установлен на компьютеры с версией ОС не ниже Windows 8/10. Для минимальной работоспособности необходимо от 6 Гбайт оперативной памяти, а также процессор с тактовой частотой не ниже 2 ГГц и 200 Мбайт свободного пространства на жестком диске.

Сертификация

Сертификация по типу ИТ.МЭ.В4.П3 (ожидается в 2022 году).

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. UserGate Management Center 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 (СОВ или IDPS). В составе UserGate NGFW присутствует собственный высокопроизводительный модуль СОВ/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 уже 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.

UserGate

Контактная информация:

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