



UserGate

Client

Обеспечение защищённого
удалённого доступа к ресурсам
корпоративной сети



UserGate Client



Обеспечение защищённого удалённого доступа к ресурсам корпоративной сети

Основное назначение продукта — обеспечение защиты инфраструктуры организации и конечных точек, соблюдение политик корпоративной безопасности внутри периметра и за его контуром.

UserGate Client осуществляет:

- проверку на соответствие политикам безопасности для конечных точек
- сбор с устройств данных о событиях информационной безопасности и телеметрии
- реагирование на угрозы информационной безопасности на конечной точке

Какие бы внешние риски ни стояли перед бизнесом, компания должна обеспечивать стабильную и непрерывную работу как сотрудников, так и корпоративных сервисов: организовывать подключение к корпоративной сети из любой точки мира и обеспечивать масштабирование своей инфраструктуры.

UserGate Client помогает решить эти и другие задачи за счёт трёх компонентов, из которых состоит продукт:

Компоненты UserGate Client

VPN¹ Целостность и передача данных без задержек	NAC³ Предоставление полной картины событий ИБ	Агент для UserGate SIEM Сбор телеметрии событий ИБ
Стабильный VPN с DTLS ² , гарантирующий безопасность данных	Расширение функциональности агентского NAC за счёт комплаенс-проверок, ZTNA ⁴ , HIP-профилирования	Связка с UserGate SIEM: быстрое реагирование на конечной точке на внешние и внутренние угрозы за счёт телеметрии

¹ VPN (Virtual Private Network, виртуальная частная сеть) — технология безопасного зашифрованного соединения поверх общедоступного Интернета.

² DTLS (Datagram Transport Layer Security) — протокол, обеспечивающий безопасность и целостность данных при высокой скорости передачи.

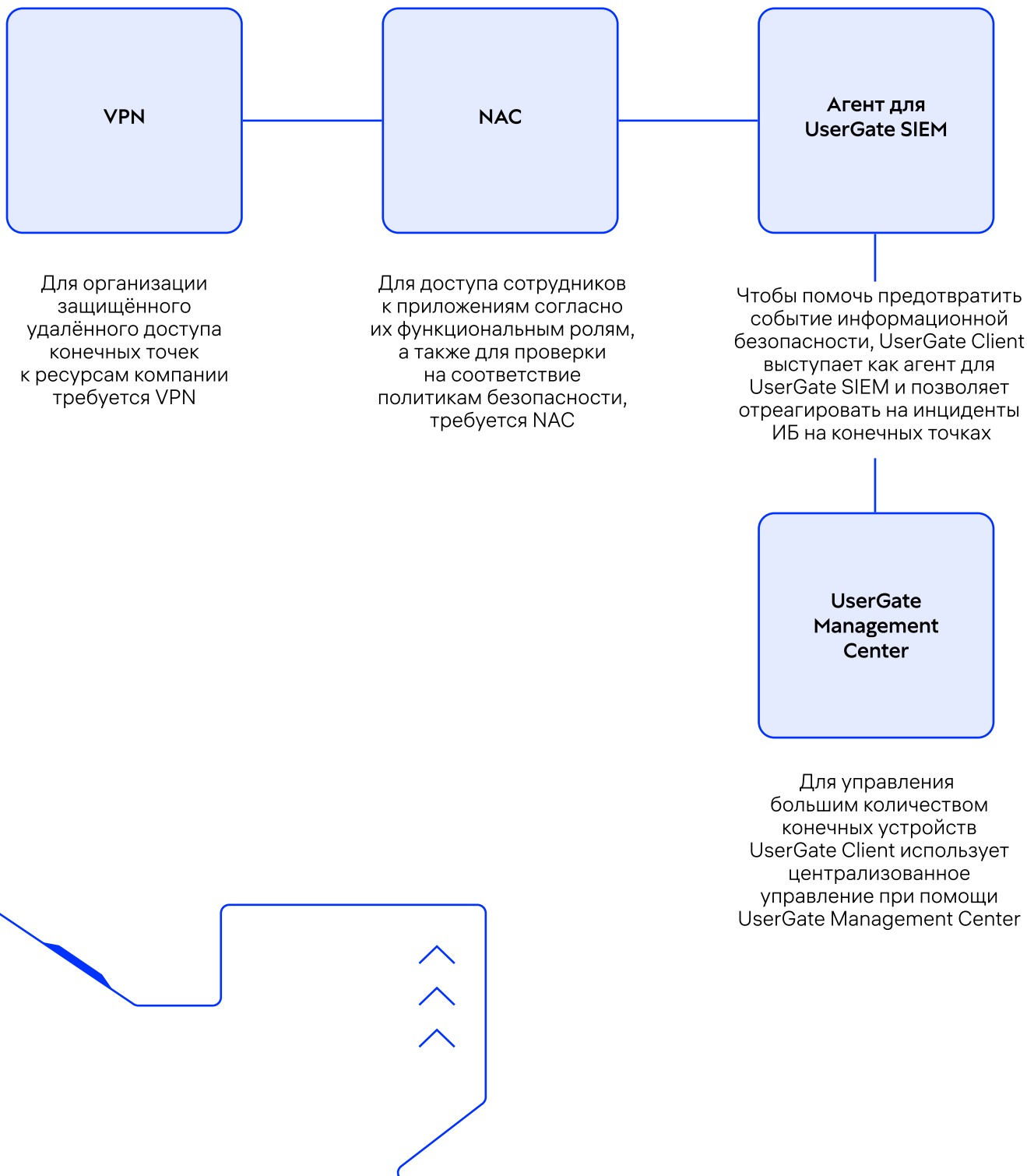
³ NAC (Network Access Control) — технология контроля доступа к сети, которая обеспечивает проверку устройств и пользователей перед подключением к корпоративной сети и во время работы в ней.

⁴ ZTNA (Zero Trust Network Access) — подход к сетевой безопасности, основанный на принципе нулевого доверия.



Принцип работы UserGate Client

Цикл, который закрывает собой продукт



Режимы работы UserGate Client

UserGate Client является неотъемлемым компонентом экосистемы UserGate SUMMA и может быть интегрирован с другими продуктами экосистемы, такими как: NGFW, Management Center, SIEM, Log Analyzer.

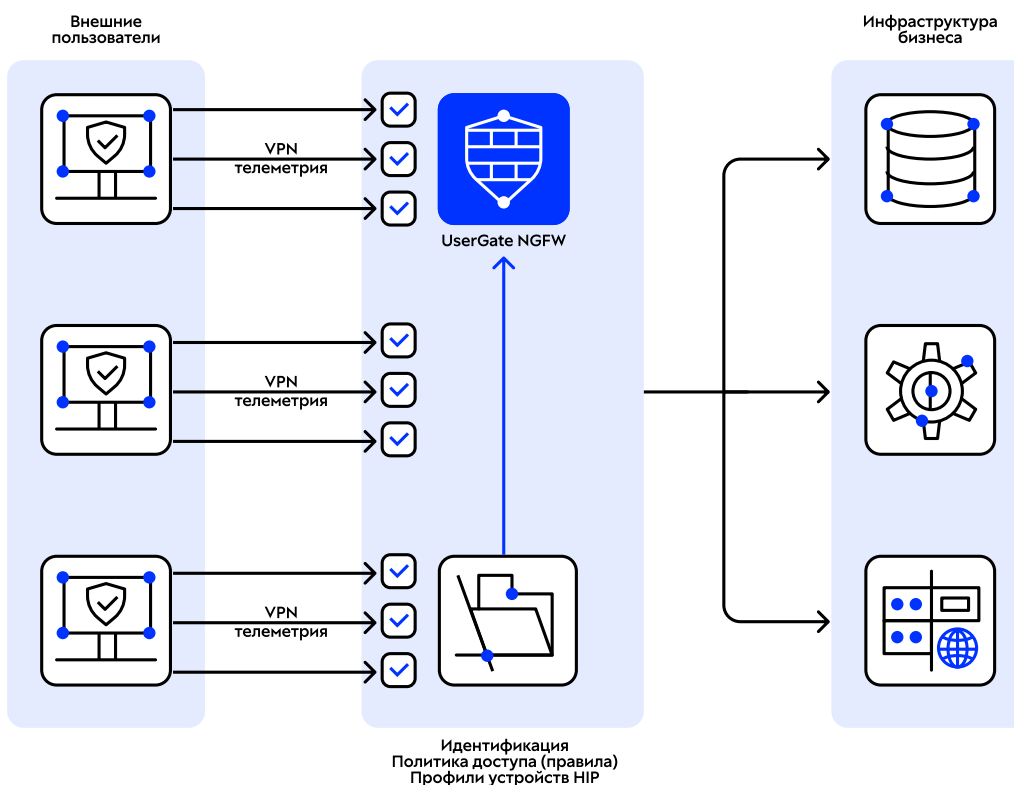
Режим работы с UserGate NGFW

Рекомендуем использовать данный режим для работы с небольшим количеством конечных точек (до 100 штук).

Возможности UserGate Client при интеграции конечного устройства с UserGate NGFW:

- защищённое VPN-подключение к UserGate NGFW. Настройка параметров VPN выполняется на конечном устройстве в окне приложения
- сбор телеметрии состояния конечного устройства на UserGate NGFW
- контроль доступа конечных устройств к сети с помощью правил межсетевого экрана на UserGate NGFW, использующих HIP-профили

Режим NGFW



Режим работы с UserGate Management Center

Рекомендуем использовать данный режим для большого количества конечных точек. Такой вариант позволит UserGate Client быстрее получить оповещение о возможном инциденте на хосте и сократить время на реагирование.

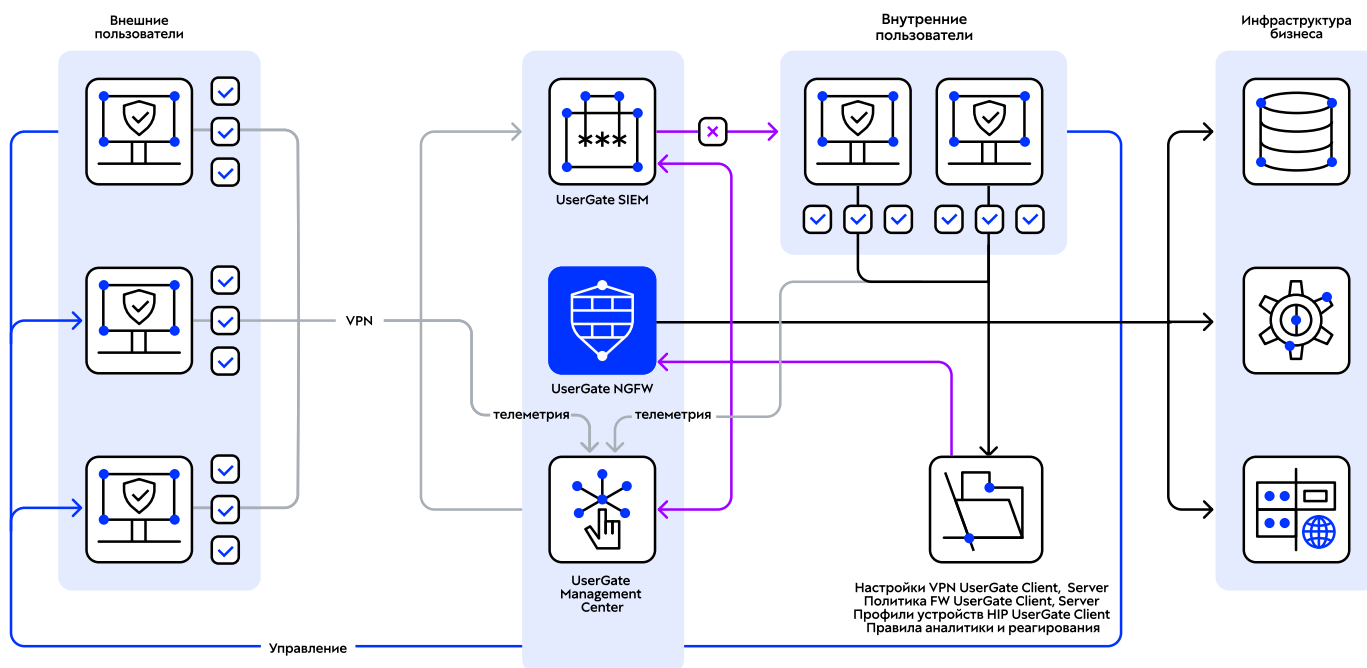
Возможности UserGate Client при интеграции конечного устройства с UserGate Management Center:

- централизованное управление конечными устройствами и их доступом в сеть без контроля доступа в соответствии с требованиями безопасности (комплаенс) с помощью HIP-профилей
- сбор телеметрии и событий безопасности с конечных устройств
- функция установления защищённого VPN-подключения: настройка параметров VPN централизованно выполняется администратором сети на UserGate Management Center и передаётся на конечное устройство

Возможности дополнительного модуля NAC для UserGate Management Center:

- проверка конечных устройств на соответствие требованиям безопасности с помощью HIP-профилей
- контроль доступа в сеть по результатам проверки на уровне конечного устройства

Режим Management Center



UserGate Client помогает решить следующие задачи

VPN

- **Безопасный удалённый доступ**

Пользователи могут безопасно подключаться к корпоративной сети вне зависимости от того, где они находятся: работают из дома, в кафе или подключаются из филиала к центральному офису.

- **Предсказуемость**

Используя UserGate Client, ИТ-отдел компании может полагаться на стабильный канал связи, что сильно упрощает планирование и поддержку устройств.

- **Удобство настройки**

Благодаря централизованному управлению через UserGate Management Center можно создавать и применять политики для VPN, ZTNA и контроля устройств из одной консоли.

- **Высокая скорость**

UserGate Client за счёт DTLS обеспечивает высокую скорость передачи данных. Это позволяет комфортно работать с ресурсоёмкими программами и поддерживать высокое качество видеоконференций.

NAC

- **Проактивная защита**

UserGate Client не позволит подключиться к корпоративной сети конечной точке, которая не соответствует политике комплаенса, — например, со старой версией антивируса или не обновлёнными базами антивирусного движка, что минимизирует риск инцидента ИБ.

- **Полная видимость**

UserGate Client даёт возможность увидеть состояние конечной точки: какие приложения запущены, какие порты открыты, какая активность ведётся.

- **Автоматизация аудита**

При использовании UserGate Client не потребуется проводить ручную проверку каждого устройства на соответствие стандартам.

- **Окупаемость инвестиций**

Агентское решение UserGate Client обеспечивает на конечных точках комплаенс-проверки, сбор телеметрии и событий ИБ, а также HIP-профилирование.

Агент для UserGate SIEM

- **Быстрое реагирование**

UserGate Client собирает детальные события информационной безопасности с каждого устройства для расследования инцидентов и проактивного поиска угроз. Это позволяет обеспечить соответствующее реагирование на инциденты ИБ.

- **Единая картина угроз**

UserGate Client предоставляет аналитикам UserGate SIEM полную картину потенциальных угроз на конечных точках.

- **Круглосуточный мониторинг активности**

Собираемые UserGate Client со всех подключённых устройств события информационной безопасности помогают выявить подозрительные действия (например, массовое копирование данных, запуск неавторизованных приложений) в любой момент работы конечной точки.

- **Сокращение времени реакции**

События информационной безопасности, которые UserGate Client собирает и передаёт в UserGate SIEM, позволяют расследовать инцидент ИБ и принять необходимые меры для реагирования с обеспечением доказательной базы.



Сценарии использования UserGate Client

VPN

Задача

Необходимо обеспечить защищённое удалённое подключение мигрирующих пользователей к ресурсам корпоративной сети из различных филиалов организации и сети Интернет (удалённая работа вне офиса).

Решение с UserGate Client

Предоставление оптимального безопасного доступа к корпоративным ресурсам по принципу Zero Trust.

Снижение нагрузки на сетевое оборудование:

- обеспечение возможности гибкой маршрутизации трафика для снижения нагрузки на сетевое оборудование и каналы связи
- разделение трафика (split tunneling): личный трафик идёт напрямую в сеть Интернет, а рабочий — через защищённое соединение

Высокий уровень безопасности при удалённом подключении:

- использование двухфакторной аутентификации или сертификатов
- защита конечной точки: встроенный межсетевой экран блокирует несанкционированные подключения прямо на устройстве сотрудника
- сквозное шифрование — все данные надёжно защищены современными протоколами

Простота управления для ИТ-отдела:

- централизованное управление предоставляет возможность гибко настраивать политики для множества пользователей из одной консоли
- поддержка российских и зарубежных ОС: единый стандарт безопасности для Astra Linux, Ubuntu, Windows

Результат

После внедрения UserGate Client организация из финансовой отрасли смогла обеспечить защищённый доступ всех сотрудников нового филиала.

В итоге:

- снизилась нагрузка на каналы подключения центрального офиса и нового филиала
- обеспечен высокий уровень защищённости за счёт применения двухфакторной аутентификации и пользовательских сертификатов
- заказчик уверенно перевёл часть своего парка устройств на отечественные ОС, зная, что совместимость с ними гарантирована UserGate Client

NAC

Задача

Удалённые устройства сотрудников и подрядчиков — слабое звено в защите инфраструктуры организации. Нет уверенности в том, что на ноутбуке установлен антивирус, включён межсетевой экран или нет нежелательного ПО. Каждое такое подключение — риск для всей сети.

Решение с UserGate Client

Автоматизация процесса проверки устройств: доступ в корпоративную сеть будет предоставлен только тем, кто соответствует политикам безопасности организации.

Использование HIP-профилей UserGate Client для проведения проверок:

- на наличие установленных критичных обновлений ОС на конечных точках
- ключей реестра, что позволит убедиться в запуске и работе важных служб ОС и СЗИ, а также в отсутствии недопустимых компонентов, добавленных в автозагрузку
- на предмет установленного антивируса и наличия у него баз, обновлённых до последних версий
- на выполнение настроек межсетевого экрана конечной точки, что позволит организовать сетевой доступ
- на включение шифрования диска для ноутбуков/конечных устройств
- на наличие установленных последних версий ПО

Гибкое управление доступом:

- разный уровень доступа для разных функциональных ролей
- возможность получить доступ к порту для обновлений в случае, если устройство не прошло проверку
- возможность масштабирования одного правила на несколько устройств

Результат

UserGate Client помог закрыть слабые места в обеспечении защищённого контролируемого подключения конечных точек к инфраструктуре организации с большим штатом сотрудников:

- отдел ИБ гарантированно снизил риски утечек данных
- отдел ИТ имеет возможность управлять политиками для множества точек через единое окно в режиме работы UserGate Client с UserGate Management Center

Агент для UserGate SIEM

Задача

При выявлении инцидента сотрудник отдела ИБ тратит много часов на поиск следующей информации:

- что произошло на оборудовании удалённого сотрудника
- какие процессы запускались
- куда были переданы данные

События информационной безопасности с конечных точек, сбор которых обеспечивает UserGate Client, служат дополнительной информацией для составления SIEM-системой полной картины произошедшего в инфраструктуре.

Решение с UserGate Client

На основании собранных событий UserGate SIEM может сформировать инцидент ИБ и отреагировать на него на конечной точке по команде оператора или в автоматическом режиме. Благодаря этому повышается защищённость как конечной точки, так и инфраструктуры организации в целом.

Как работает агент для SIEM

Сбор событий ИБ — это ключевые данные для расследования. Такими событиями могут быть:

- внедрение вредоносного программного обеспечения в процессы ОС и установленное ПО
- получение несанкционированного доступа
- внесение изменений в конфигурацию ОС
- несанкционированное использование внешних устройств и другие нарушения ИБ

Быстрое обнаружение и реагирование:

- изоляция устройства при обнаружении инцидента с помощью UserGate SIEM
- ограничение доступа за счёт перевода пользователя в «карантинную зону»

Результат

За счёт интеграции двух решений — UserGate SIEM и UserGate Client в режиме работы с UserGate Management Center — значительно сокращается время на реагирование и расследование инцидента. Отдел ИБ получает механизм, который повышает защищённость организации и снижает потенциальный ущерб от инцидентов.





Технические параметры

Поддержка ОС: Windows, Linux (VPN)

В 2026 году планируется расширение поддержки ОС семейства macOS, а также ОС семейства Linux, в том числе отечественных.

Поддерживаемые технологии

VPN, протоколы TLS и DTLS, IPsec VPN (IKEv2), Split tunneling, Remote Access VPN.

Аутентификация и авторизация

Поддержка LDAP-коннектора, Radius, TACACS+, Kerberos, NTLM, SAML (SSO), 2FA (TOTP) и MFA.

Централизованное управление

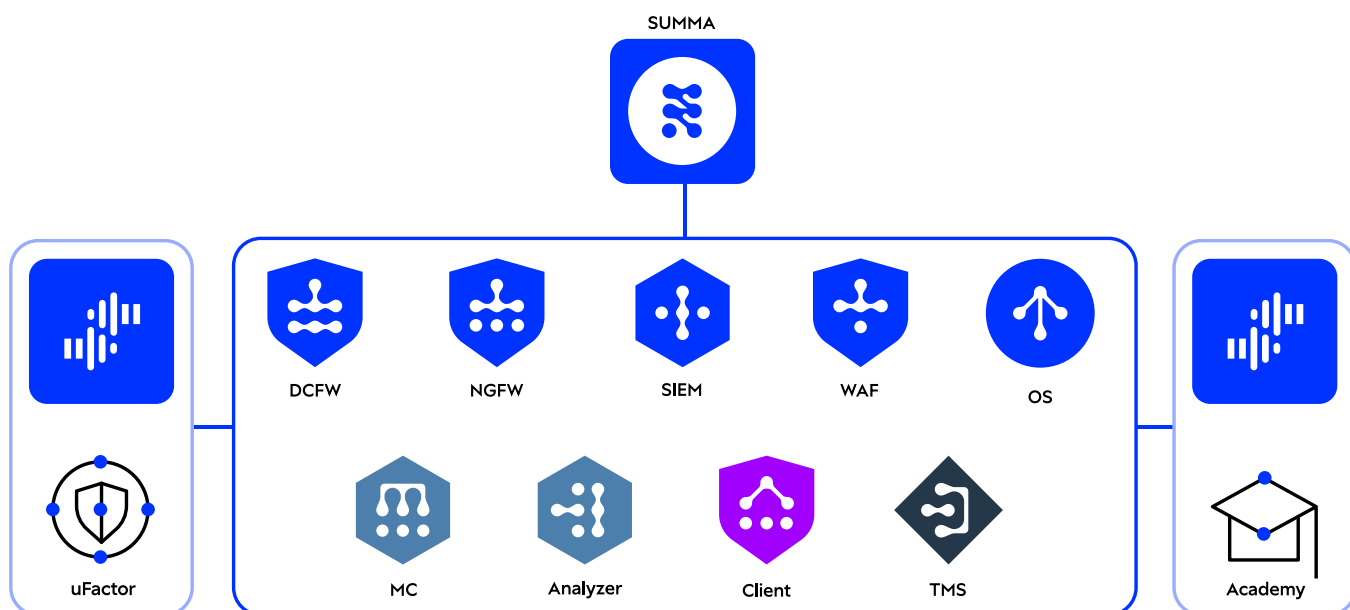
Управление политиками, пользователями и устройствами осуществляется через единую консоль UserGate Management Center.

Совместимость

UserGate Client работает в связке с продуктами экосистемы UserGate SUMMA: с UserGate NGFW и UserGate Management Center — для сбора логов и событий информационной безопасности; с UserGate SIEM и UserGate Log Analyzer— для их хранения.



Интеграция с продуктами экосистемы безопасности UserGate SUMMA



UserGate Client является необходимым компонентом экосистемы и работает в связке с другими продуктами SUMMA:

- Для централизованного управления из единой точки парком рабочих станций используется режим подключения UserGate Client к UserGate Management Center (MC). В этом режиме UserGate Client сообщает администратору экосистемы UserGate SUMMA данные о состоянии конечных устройств, включая информацию о запущенных приложениях, обновлениях, версиях ПО, загрузках процессора, критических событиях на устройстве, журналах различных сервисов и других параметрах
- Телеметрическая информация, журналы Windows и другие данные о безопасности конечных устройств, полученные от UserGate Client, передаются в систему мониторинга UserGate SIEM и могут быть использованы для автоматического реагирования на угрозы безопасности
- Интеграция UserGate Client с UserGate NGFW, Management Center и SIEM позволяет гибко проводить централизованную настройку большого количества конечных точек, обеспечивать защиту компьютера и соблюдать политики корпоративной безопасности при выходе за защищённый периметр организации

Взять на тест UserGate Client



Контактная информация:

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

Полезные ресурсы UserGate:

