Новинки компании UserGate в информационной безопасности

Содержание:

1. Экосистема UserGate SUMMA.
2. UserGate NGFW 6.
3. UserGate FG.
4. UserGate АСУ ТП.
5. UserGate Client.
6. UserGate LogAn.
7. UGaaS (UserGate as a Service).

Компания UserGate хорошо известна как производитель отечественных программно-аппаратных комплексов по межсетевому экранированию. И совсем недавно она провела большую конференцию. Я побывал на этом мероприятии и хочу рассказать обо всех новинках как в программном обеспечении, так и в аппаратной части устройств, которые были представлены на нем.

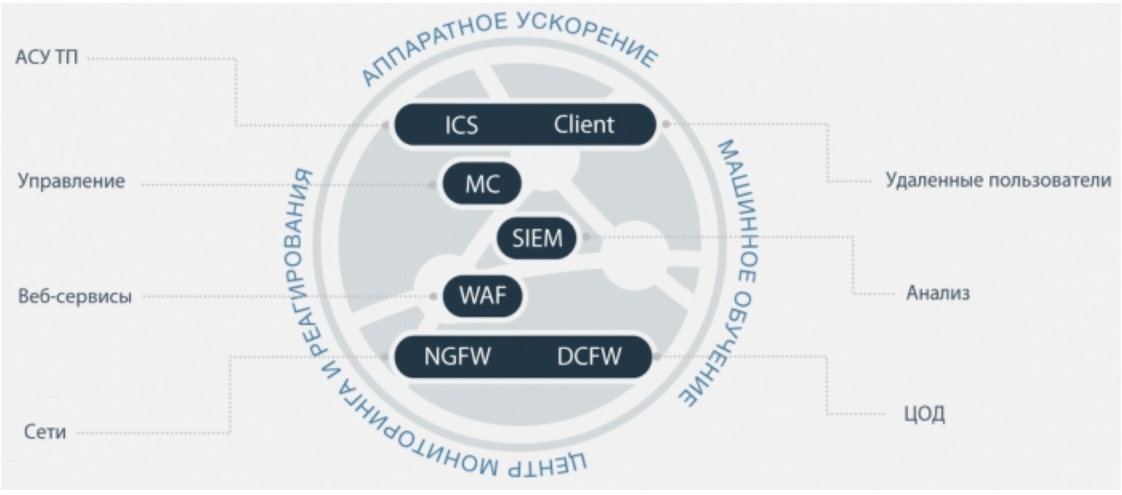
А теперь обо всем по порядку.

Экосистема UserGate SUMMA

Компания UserGate представляет новое видение защиты информации: использование комплексного решения – так называемой, экосистемы SUMMA.

Своим названием решение обязано СУММе всех компонентов, которые сейчас есть у UserGate и которые выйдут в скором времени. Решение будет включать в себя продукты для защиты стандартных сетей (NGFW), ЦОД (DCFW), АСУ ТП (ICS). Будет содержать продукты для защиты веб-сервисов (WAF), удаленных пользователей (Client). А также приложения для анализа (SIEM) и управления (MC) всей системой продуктов UserGate.

Кроме того, в компании UserGate помимо уже существующих отечественных разработок в программном обеспечении, добавились собственные аппаратные разработки. Теперь платформы серии X и C будут поставляться в отечественном корпусе, и скоро к этому списку добавится платформа серии D. Но об этом чуть попозже.



UserGate NGFW 6

Решение UserGate NGFW (Next Generation Firewall) является ключевым элементом в экосистеме UserGate SUMMA. В связи с этим, межсетевой экран шестого поколения получил множество обновлений и дополнительных функций.

Что нового появилось в UserGate NGFW 6:

1. Поддержка UserGate Management Center. Management Center - это центральная консоль управления парком оборудования UserGate. К его преимуществам можно отнести:

a. Возможность управления не только межсетевыми экранами, но и всеми решениями UserGate, находящимися в системе.

b. Возможность управления устройствами, которые находится в разных организациях, например "дочках" основной компании.

c. Появились группы шаблонов, которые позволяют производить удобную настройку парка оборудования с одного устройства.

d. Возможность управлять обновлениями всех устройств UserGate.

2. Добавились новые сетевые функции:

a. Поддержка VRF - реализация нескольких виртуальных маршрутизаторов на базе одного физического. Каждый виртуальный маршрутизатор может иметь свою таблицу маршрутизации.

b. Multicast маршрутизация -- многоадресная рассылка от одного отправителя ко многим получателям, например для IPTV.

c. Поддержка протокола маршрутизации RIP.

3. Поддержка работы с Cisco VPN при подключении к маршрутизаторам Cisco.

4. Добавление нового собственного более производительного движка - СОВ (производительность увеличена до 10 раз). Доработка профиля SSL. Добавление ГОСТ TLS. Добавление функции инспектирования каналов SSH.

5. Добавление новых протоколов для работы с АСУ ТП. Возможность обработки зеркального трафика.

6. Повышена производительность отдельных компонентов:

a. Сетевых функций.

b. Идентификации пользователей.

c. Интернет фильтрации.

d. Защиты от угроз.

7. Поддержка SSL Broker, что позволяет отдавать расшифрованный SSL трафик на сторонний сервис.



UserGate FG

Также, компанией UserGate анонсирован выход нового продукта - межсетевого экрана для ЦОД (DCFW).

Целевыми заказчиками данного продукта компания видит:

1. Государственные, отраслевые и коммерческие ЦОДы.
2. Операторы связи, нуждающиеся в:

a. Построении новых каналов связи.

b. Развитии инфраструктуры для 5G сетей.
c. Обработке повышающегося объема данных.

Разработкам предшествовало изучение рынка. Как выяснилось, максимальная производительность у подобных решений доходит до 80 Gb/s при использовании межсетевого экрана уровня L4. Причем, реальная производительность этих систем зачастую менее 300 тыс пакетов в секунду. В итоге, получается дорогое и малопроизводительное решение для датацентров.

Если посмотреть на зарубежные решения, то среди них можно найти и более производительные модели. Но следует иметь ввиду, что, начиная с 2024 года, у всех зарубежных решений будут большие сложности с сертификацией в России. А значит, размещение их на своей сети будет связано с определёнными трудностями.

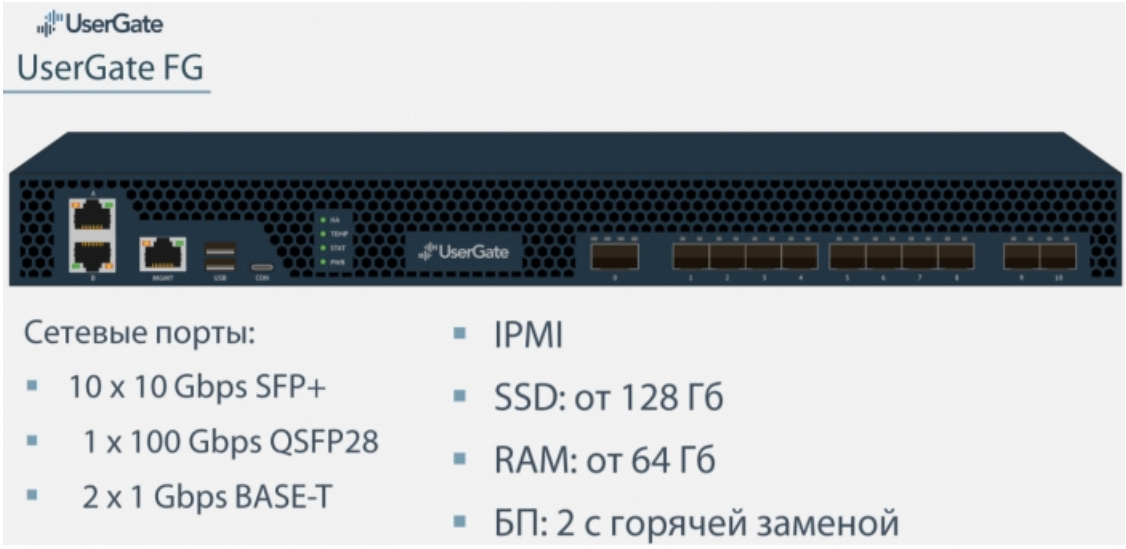
В связи со всеми вышеизложенными моментами, компания UserGate решила вывести на рынок свой продукт для уровня ЦОД - межсетевой экран с аппаратным ускорением UserGate FG.

Его отличительными особенностями являются:

1. Аппаратная обработка трафика на ПЛИС. Это отдельный процессор с заранее загруженными в него правилами межсетевого экрана, фильтрации и т.д.
2. Производительность более 80Gb/s на пакетах в 64 байта – это трафик, который наиболее приближен к пакетам реальных приложений.
3. Обработка до 120 миллионов пакетов в секунду (по сравнению с 300 тыс у конкурентов).
4. Это решение уровня "Wire speed" – скорость межсетевого экрана равняется скорости сетевого интерфейса.
5. Полностью собственная разработка.
6. Включение данного решения в реестр Минпромторга.

Состав межсетевого экрана UserGate FG:

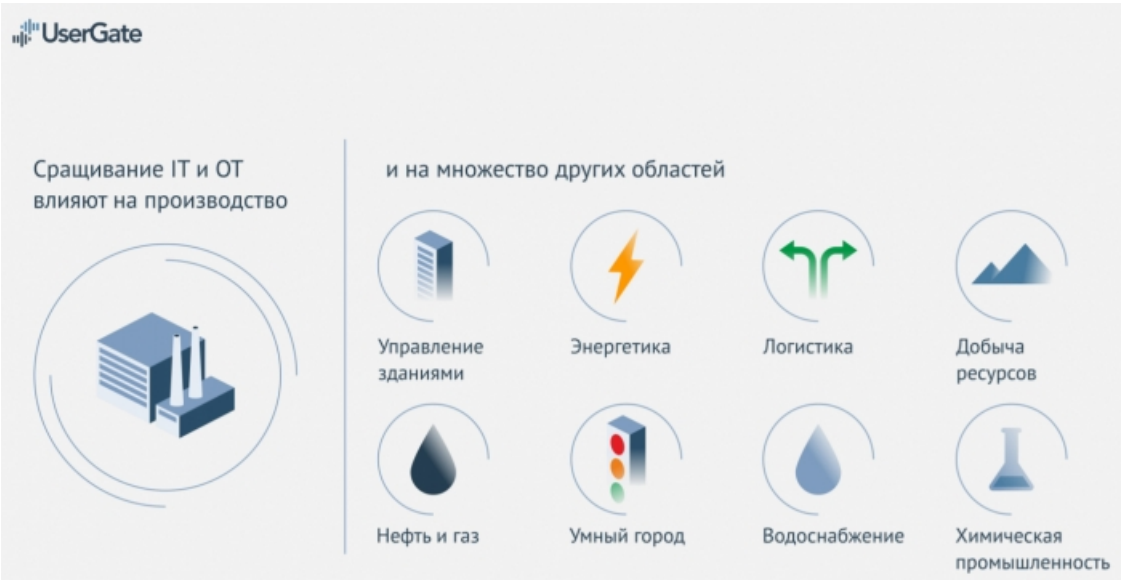
1. 10 портов SFP+ со скоростью подключения 10 Gb/s на каждом.
2. 1 порт QSFP28 со скоростью подключения 100 Gb/s для аплинка.
3. 2 порта Base-T (медных) со скоростью подключения 1 Gb/s для объединения данного решения в кластер из нескольких железок. Кластер поддерживает как режим работы active-passive (для повышения отказоустойчивости), так и режим active-active (для повышения производительности).
4. 1 порт Base-T со скоростью подключения 1 Gb/S для для удаленного управления (IPMI).
5. Встроенный SSD объемом от 128GB.
6. Оперативная память объемом от 64GB.
7. 2 блока питания с функцией горячей замены.



Даже учитывая достаточно большую производительность первой версии решения на данный момент, компания UserGate видит перспективы его развития. В следующей версии к UserGate FG планируется добавить движок системы обнаружения и предотвращения вторжения (IPS), а также систему контроля приложений на уровне L7. Что, в итоге, позволит получить полноценный NGFW, производительность которого будет превышать 80Gb/s.

UserGate АСУ ТП

Сращивание IT и АСУ ТП сетей несет в себе такие плюсы, как ускорение бизнес-процессов, оптимизация планирования, упрощение взаимодействия с контрагентами и т.д. Но также, данный процесс имеет и отрицательную сторону. Сращивание ставит под угрозу такую сеть, и открывает дополнительные возможности для злоумышленников.



Обычно, АСУ ТП сети проектируются на много лет, поэтому они имеют свойство технически устаревать до вывода из эксплуатации оборудования, что ведет за собой снижение надежности и защищенности такой сети. Основным критерием для сети АСУ ТП является непрерывность работы, иногда даже в ущерб конфиденциальности какой-либо информации.

UserGate может реализовать отказоустойчивый кластер, что в совокупности с тегированным трафиком для сегментации сети дает возможность организовать надежную сеть АСУ ТП, отделенную логически (не физически) от обычной корпоративной сети.

Еще одной особенностью является возможность прозрачного внедрения решения UserGate в разрыв сети, с обеспечением всего необходимого функционала: файрвол, детектирование сотен приложений и протоколов уровня L7, покомандный разбор и применение политики на уровне каждой команды. Возможность обработки зеркального трафика позволяет проводитьанализ безопасности, не вторгаясь в технологический процесс.

Также, сети АСУ ТП зачастую имеют повышенные требования к условиям работы оборудования. Сюда входят высокие температуры, повышенная влажность, электромагнитное взаимодействие и т.д. Специально для этих целей компания UserGate разработала продукт UserGate X1, который рассчитан на работу в самых суровых условиях: при температурах от -40С до +70С и относительной влажности от 5% до 95%. Модель имеет компактный размер, вес около 1 кг и настенное крепление или крепление на DIN-рейку. Все это делает возможным ее применение для защиты промышленных, транспортных и других объектов, расположенных на открытом воздухе.

Ниже представлены фотографии межсетевых экранов серий X и C, которые являются собственной разработкой компании UserGate, выполненной с учетом собранных отзывов и пожеланий заказчиков.

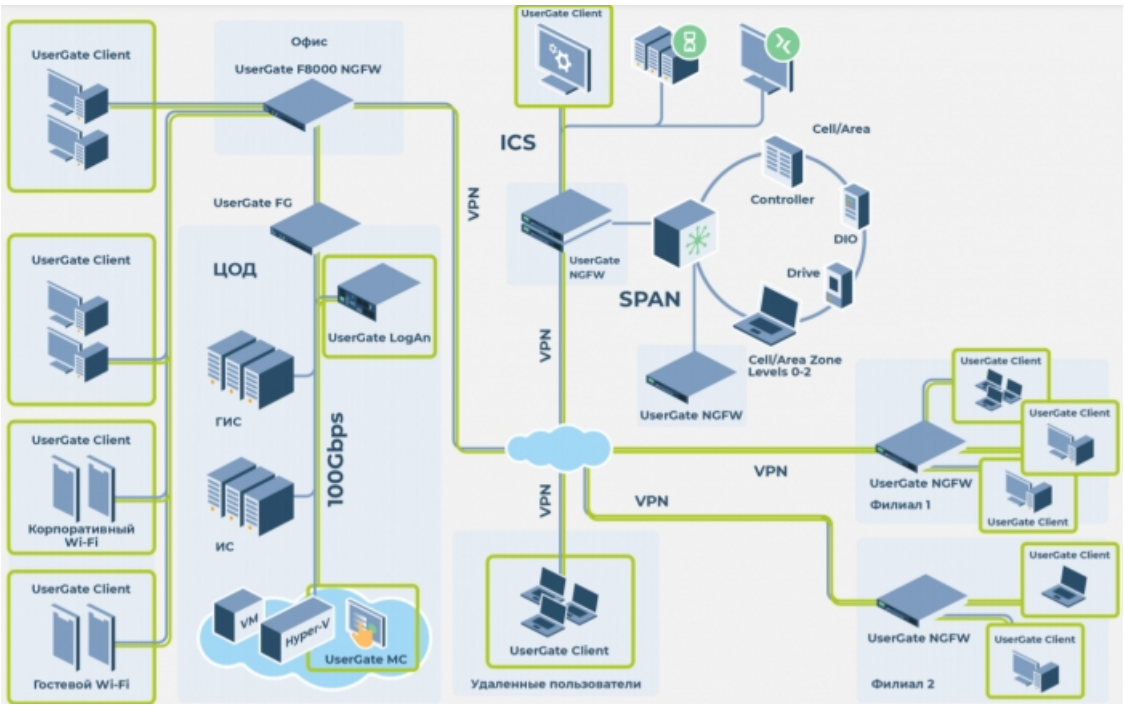


UserGate Client

UserGate Client является пока что концептом программного обеспечения для конечных устройств. В своей основе он имеет технологию EDR, которая отвечает за расширенное обнаружение и предотвращение атак.

Что даст заказчику решение UserGate Client:

1. Позволит видеть инфраструктуру целиком, понимать что происходит на каждом устройстве и выделять важные события.
2. Позволит определять сложные угрозы на устройствах.
3. Позволит получать расширенную информацию об устройстве в системе.
4. Позволит автоматизировать процессы безопасности.



На картинке выделены примеры мест использования решения UserGate Client. Это конечные устройства в различных частях сети, будь то основной офис, филиалы, удаленные пользователи, рабочее место АСУ ТП и т.д.

Решение UserGate Client используется вместе с решениями Management Center и Log Analyzer, для упрощения отслеживания инцидентов и администрирования.

Также, помимо стандартных функций EDR, UserGate Client имеет функции:

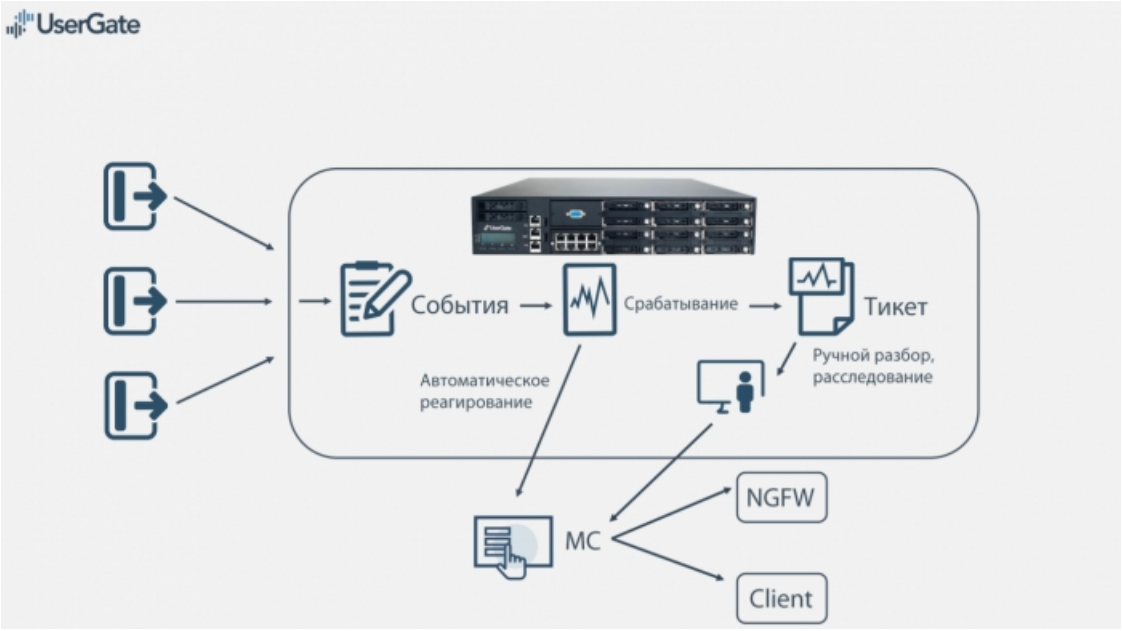
1. Межсетевого экрана.
2. Дополнительного уровня аутентификации.
3. VPN клиента для организации безопасного удаленного доступа.

UserGate LogAn

UserGate Log Analyzer или LogAn, изначально имел функцию только анализа логов. Сейчас к нему добавилось множество новых функций:

1. Реагирование на события.
2. Правила аналитики для упрощения работы с логами
3. Настройка автоматического реагирования на определенные инциденты. К ним относится отправка EMAIL писем, SMS сообщений, блокировка хоста/адреса и т.д.
4. Инструмент для разбора инцидентов (тикетов) с множеством различных функций.
5. Получение логов с любого сетевого устройства по протоколу SNMP.
6. Правила для формирования различных отчетов.
7. Подключение к Windows машинам по технологии WMI.
8. Подключение всей линейки оборудования UserGate.
9. Темная тема в интерфейсе управления (по просьбе пользователей).

Если описать коротко, то UserGate LogAn - это унифицированная платформа с помощью которой происходит сбор, аналитика, срабатывание, разбор инцидента и формирование правил для дальнейшей работы с подобными инцидентами.



В результате, все нововведения превращают UserGate LogAn в полноценную SIEM-систему с функциями IRP. А совокупность UserGate LogAn и Management Center дает возможность реализовать концепцию SOAR (реакция на инциденты и проактивная защита).

UGaaS (UserGate as a Service)

UserGate предоставила возможность всем заказчикам, невзирая на их размер, получить качественный сервис по защите их инфраструктуры. Речь, конечно же, о подписочной модели UserGate as a Service (как услуга).

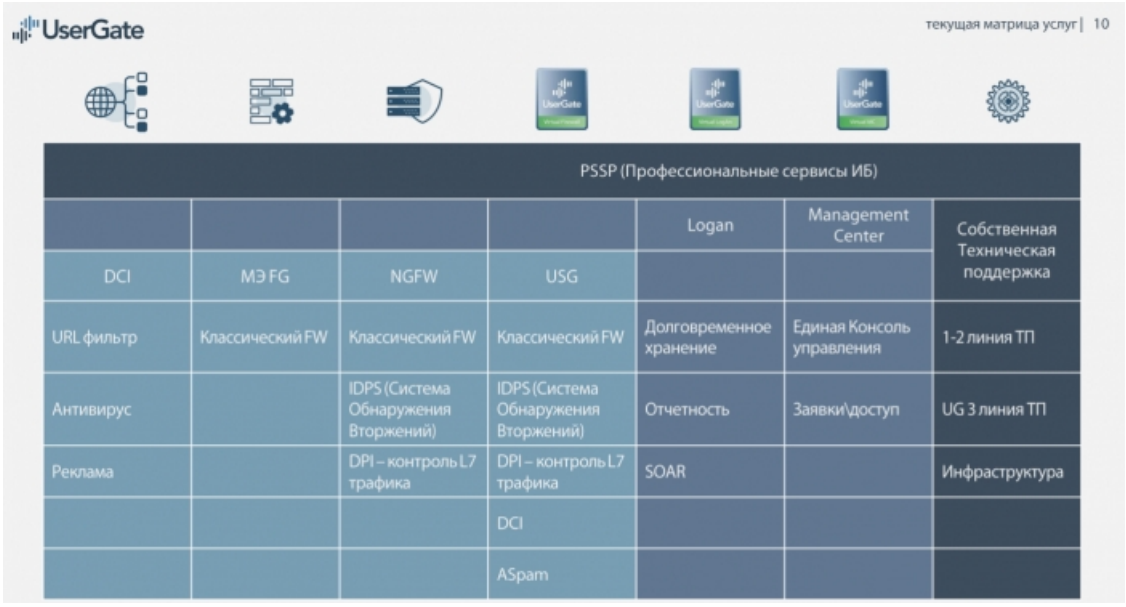
Для кого данный сервис может быть актуальным:

1. Малый и средний бизнес (SMB).
2. Отраслевые ГК (РосАтом, РосТех, РЖД и т.д.).
3. Распределенные Государственные структуры
4. Сетевые провайдеры.

UserGate готовы предлагать виртуальные устройства для обеспечения услуг информационной безопасности (MSSP). Этот сервис может быть реализован как на аппаратной платформе UserGate, так и на сторонней платформе, подходящей по характеристикам или в выделенной среде виртуализации. В качестве примера, виртуального шлюза безопасности с 32 ядрами будет достаточно для обслуживания организации с 6-8 тысячами виртуальных пользователей.

Список пакетов, которые предоставляет UserGate:

1. Пакет "Контентная фильтрация". Он подойдет для операторов и сервис-провайдеров, которые заинтересованы в ограничении доступа своих пользователей к паразитным категориям контента или вредоносного трафика.
2. Пакет "Классический межсетевой экран". Включает в себя как функции пакета контентной фильтрации, так и систему обнаружения вторжения и функцию приоритезации трафика.
3. Полный пакет "Шлюз безопасности". Ко всему вышеперечисленному добавляется сбор статистики, центр управления системой и техническая поддержка всех сервисов UserGate.



Компания UserGate описала три схемы реализации данного сервиса:

1. Схема "Мультиаренда". Разворачивается шлюз безопасности от UserGate, который занимается очисткой всего трафика в канале. Подойдет для частных пользователей и небольших корпоративных заказчиков.
2. Схема "Выделенное виртуальное устройство". Подписчику выделяется отдельное устройство для самостоятельного управления или управления профессиональным сервис-провайдером. Подойдет для тех, кто не может использовать облачные ресурсы и вынужден внедрить систему в локальную сеть.
3. Схема "Срвис-провайдер". Подойдет для провайдеров с локальным или облачным пулом заказчиков. В данной схеме для каждого заказчика разворачивает свой домен устройств UserGate.

Все продукты компании UserGate доступны для приобретения по подписке (как сервис), за тисключением аппаратных средств. Также, компания UserGate заверяет, что готова для каждого проекта подходить к формированию цены продукта как сервиса в индивидуальном порядке.

Заключение

Хотелось бы отметить, что новинок, представленных в этом году компанией UserGate, оказалось рекордное количество. Добавили и производительности в ПО, и продукты для решения новых задач, и даже свои аппаратные разработки.

Думаю, можно заранее сказать, какие представленные продукты компании UserGate точно будут пользоваться популярностью среди заказчиков - это UserGate DCFW (FG) и UserGate Client.

Межсетевой экран для датацентров позволит большому потоку трафика "очищаться" по первичным правилам, тем самым снимая лишнюю нагрузку с каналов связи, и устранять большую часть вредоносного контента, что является очень востребованным в рамках обработки большого объема данных.

Клиентское ПО для защиты информации пользуется большой популярностью и спросом среди заказчиков. Сразу заявлю, что продукт UserGate Client не сможет, да и наверно не захочет, претендовать на стандартные розничные продажи. Это решение, которое хорошо дополнит имеющуюся инфраструктуру с оборудованием UserGate, но не будет актуально при использовании в одиночку.

Еще хочу отметить решение, под которое наш рынок еще не до конца сформирован - UGaaS (UserGate as a Service). Нашему рынку еще предстоит пройти "преображение" в течении нескольких лет, для популяризации "решений как услуги". После чего мы действительно сможем наблюдать повышенный спрос на такой продукт.