Межсетевой экран UserGate

До 2010 года

Компания Entensys разрабатывала популярные программные решения под Windows-платформу для малого и среднего бизнеса (более 50 тысяч организаций)

2010 год

Произошла смена стратегии, началась разработка кроссплатформенного решения нового поколения, в том числе адаптированного для использования в виртуальных средах

2013 год

Был выпущен UserGate Web Filter, который стал использоваться крупнейшими операторами связи и провайдерами публичного WiFi, университетами, школами (около 14 тысяч школ)

2016 год

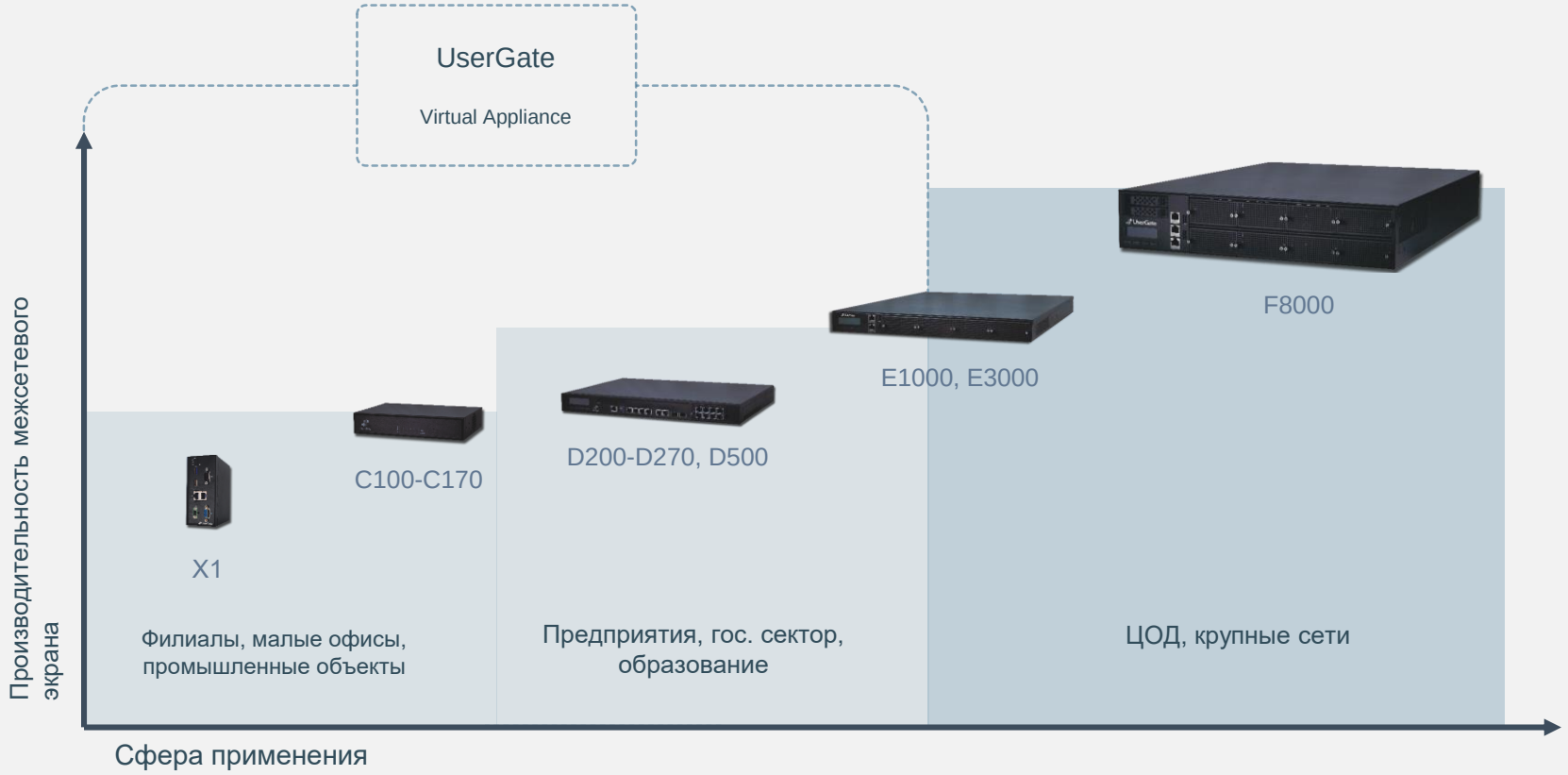
Выпущен UserGate UTM, комплексное решение по интернет-безопасности, разработанное как развитие уже опробованной на сетях операторов связи платформы

Настоящее время

Ребрендинг UserGate — универсальный шлюз безопасности

- Не уступает мировым лидерам
- Активное развитие партнерской сети/площадки сертификации
- Сертификат ФСТЭК России
- Участник проекта ГосСопка Импортозамещение

Работа решений линейки UserGate основана на одноименной платформе, доступной в виде виртуального решения (готового образа для VMware, Hyper-V и прочих систем виртуализации) или в виде appliance, то есть программно-аппаратного комплекса



	UserGate C	UserGate D	UserGate E	UserGate F	UserGate X
Appliance					
FW, Гбит/с	До 1	18-20	25-30	40	0,3
IPS (COB), Мбит/с	100	500-700	1200-1500	4200	10
ATP, Мбит/с	50	300-350	400-600	2800	15
Контроль Приложений L7, Мбит/с	70	700-800	1000-1400	3200	15
Антивирус Касперского , Мбит/с	20	240-260	300-500	1000	8
Максимальное рекомендованное количество сессий	100	300-500	1000-3000	10000	-

Здравоохранение

Банки
и финансовые
организации

Горнодобывающая
промышленность

Наука

Энергетика
и топливно-
энергетический
комплекс

Транспорт

Металлургическая
промышленность

Сфера атомной
энергии

Химическая
промышленность

Связь

Ракетно-
космическая
промышленность

Оборонная
промышленность

01

Филиалы, POS-системы, ритейл

VPN, МСЭ, СОВ, антивирус, антиспам

02

Предприятия, гос. сектор

МСЭ, Управление пользователям, управление трафиком, прокси-сервер

03

ЦОД, крупные сети

МСЭ, СОВ, антивирус UserGate, отказоустойчивость

04

Образовательные учреждения

контентная фильтрация, публичный WI-FI, соответствие требованиям № 139-ФЗ и № 436-ФЗ

05

Объекты на открытом воздухе

VPN, МСЭ, СОВ, антивирус, SCADA

Защита от угроз
(Threat protection)

Межсетевой экран
(Enterprise Firewall, NGFW)

Анализ угроз
(Поддержка концепции SOAR)

Операционная
система UGOS

Интернет-
фильтрация
(Internet filtering)

Защита от атак,
безопасность
дата-центров
(IPS)

Виртуальная
частная сеть
(VPN)

Безопасность почты
(Mail Security)

Высокая отказоустойчивость
и кластеризация
(High Availability and Clustering)

Поддержка АСУ ТП
(SCADA)

Контроль доступа
в интернет

Гостевой портал

NEW
Центральная
консоль

Контроль приложений
на уровне L7

Безопасная
публикация ресурсов
и сервисов

Идентификация
пользователей

NEW
UserGate
Log Analyzer

Дешифрование
SSL

Антивирусная
защита

Контроль мобильных
устройств, поддержка
концепции BYOD

Личный кабинет

My.Usergate.com (документация, образы для скачивания)

Функционал решения UserGate

https://www.usergate.com/ru/products

Политика лицензирования

https://www.usergate.com/ru/purchase

Сертификат ФСТЭК России

http://static.entensys.com/docs/UserGate-FSTEC-3905.pdf

Варианты исполнения: аппаратные комплексы

https://www.usergate.com/ru/products

Virtual Appliance

https://www.usergate.com/ru/products/usergate-vm

UserGate для **учреждения здравоохранения**

https://www.usergate.com/ru/solutions/healthcare

UserGate для **учреждений образования**

https://www.usergate.com/ru/solutions/education

Политика UserGate **государственным структурам**

https://www.usergate.com/ru/solutions/government

UserGate **промышленным предприятиям**

https://www.usergate.com/ru/solutions/industrial

UserGate **малому и среднему бизнесу**

https://www.usergate.com/ru/solutions/smb

UserGate для **субъектов КИИ**

https://www.usergate.com/ru/solutions/critical-infrastructure

UserGate работает на базе специально созданной и поддерживаемой операционной системы, а также на специально спроектированных аппаратных устройствах, позволяющих обеспечить наибольшую эффективность и скорость обработки трафика.

Разработчики уделили много внимания созданию собственной платформы, не основанной на использовании чужого исходного кода и сторонних модулей.

Что позволяет обеспечивать высокое качество работы продукта, а также его скорейшее развитие и адаптацию для самых сложных проектов.

NGFW - Next Generation Firewall
должен обеспечивать:

- Высокую скорость обработки трафика
- Применением гибких политик к пользователям
- Контроль приложений на L7 уровне по всем портам
- Интернет-фильтрацию, инспекцию SSL-трафика
- Идентификацию пользователей
- Антивирусную защиту

Технологии, используемые в UserGate, соответствуют современной концепции SOAR (Security Automation, Orchestration and Response), позволяют анализировать поведение различных процессов, выявлять риски и автоматически обеспечивать на основе этого анализа адекватную реакцию, обеспечивая защиту от угрозы или просто от аномального поведения на самой ранней стадии

Аутентификацию пользователей и применение к пользователям правил межсетевого экранирования, контентной фильтрации, контроля приложений с поддержкой таких средств и протоколов аутентификации, как Active Directory, Kerberos, RADIUS, LDAP, Captive Portal, TACACS+, MFA.

Администраторы могут применить определенные политики безопасности к любому пользователю, группе пользователей или, например, ко всем неизвестным пользователям.

Анализ поведение различных процессов, выявление рисков и автоматическое обеспечиваемая на основе этого анализа реакция, для защиты от угрозы или просто от аномального поведения на самой ранней стадии.

UserGate позволяет обеспечить гостевой интернет-доступ через Wi-Fi. При этом поддерживаются различные методы аутентификации – в том числе по одноразовому паролю, а также через SMS.

Возможно применение к гостевым пользователям специальных политик и правил, обеспечение мониторинга использования интернета и получение данных статистики.

В обновленной версии операционной системы UGOS появилась возможность настройки автоматизированной системы управления технологическим производством (АСУ ТП, SCADA) и управления ей. Таким образом, администратор может контролировать трафик, настроив правила обнаружения, блокировки и журналирования событий.

Это позволяет автоматизировать основные операции технологического процесса, сохраняя при этом возможность контроля и вмешательства человека при необходимости.

Контроль работы веб-приложений и доступа в интернет с помощью создания правил, основанных на персонализированной политике. Это обеспечивает разноуровневый доступ к сетевым ресурсам и позволяет распределять ширину канала между различными приложениями и сервисами.

Функция контроля доступа в интернет также позволяет автоматически применять настройки безопасности к отдельным пользователям и объектам сетевой инфраструктуры.

В UserGate предоставляет различные способы обеспечения антивирусной проверки трафика.

Антивирус UserGate, включаемый в дополнительный модуль Advanced Threat Protection, обеспечивает быструю проверку трафика на наличие вредоносного кода путем анализа сигнатур получаемых файлов и приложений. Данный метод антивирусной проверки практически не влияет на производительность системы.

Встроенный антивирусный модуль с эвристическим анализом предоставляет более сложную проверку трафика.

Функция контроля приложений (на уровне L7) на основе обновляемых баз сигнатур может быть использована в правилах межсетевого экрана и правилах пропускной способности. Это обеспечивает защиту от угроз, связанных с программами, имеющими доступ в интернет.

Данная функции с одной стороны позволяет администраторам ограничивать использование таких приложений, как мессенджеры или торрент-клиенты,
в личных целях, с другой - защитить локальную сеть от связанных с интернетом угроз.

Защита от угроз нулевого часа
В платформе UserGate используются технологии поведенческого анализа, оценка репутации всевозможных ресурсов, доступ к базам сигнатур известных вредоносных программ, а также «песочницам».

Защита от DoS-атак
На базе платформы UserGate возможно обеспечить защиту от DoS-атак, в том числе ограничивая максимальное число соединений на одного пользователя.

Блокировка рекламы
UserGate анализирует загружаемый контент с учетом знания известных рекламных сетей и используемых ими скриптов.

Разбор и анализ трафика
UserGate осуществляет морфологический анализ содержимого веб-страниц
на наличие определенных слов и словосочетаний (Web 2.0)

Функция высокой отказоустойчивости (High Availability) позволяет кардинально снизить риски, которые могут возникать в связи со сбоями в работе аппаратного обеспечения, на котором установлен UserGate. Данная функция позволяет устанавливать систему на парных узлах и автоматически переключать между ними нагрузку в случае сбоев. В решении реализована поддержка кластеризации в режиме active-active и active-passive. Кластеризация позволяет применять к разным нодам единые настройки, политики, библиотеки, сертификаты, сервера авторизации, группы пользователей и т. д.

Проверка почты важна как для фильтрации спама, так и для защиты от зараженных писем, фишинга, фарминга и прочих видов мошенничества. UserGate позволяет отфильтровывать письма, основываясь на анализе их содержания и эвристике.

При этом обеспечивается практически нулевой уровень ложной детекции. Центр обнаружения спама выявляет спамерские атаки в любой точке мира.

Использование интернет-фильтрации значительно увеличивает безопасность локальной сети, так как позволяет обеспечить административный контроль за использованием интернета, закачками и обеспечивает блокировку посещения потенциально опасных ресурсов, а также, когда это необходимо, сайтов, не связанных с работой.

UserGate получил ряд наград именно за качество интернет-фильтрации и широко используется для этой цели во многих организациях, вузах и у операторов связи.

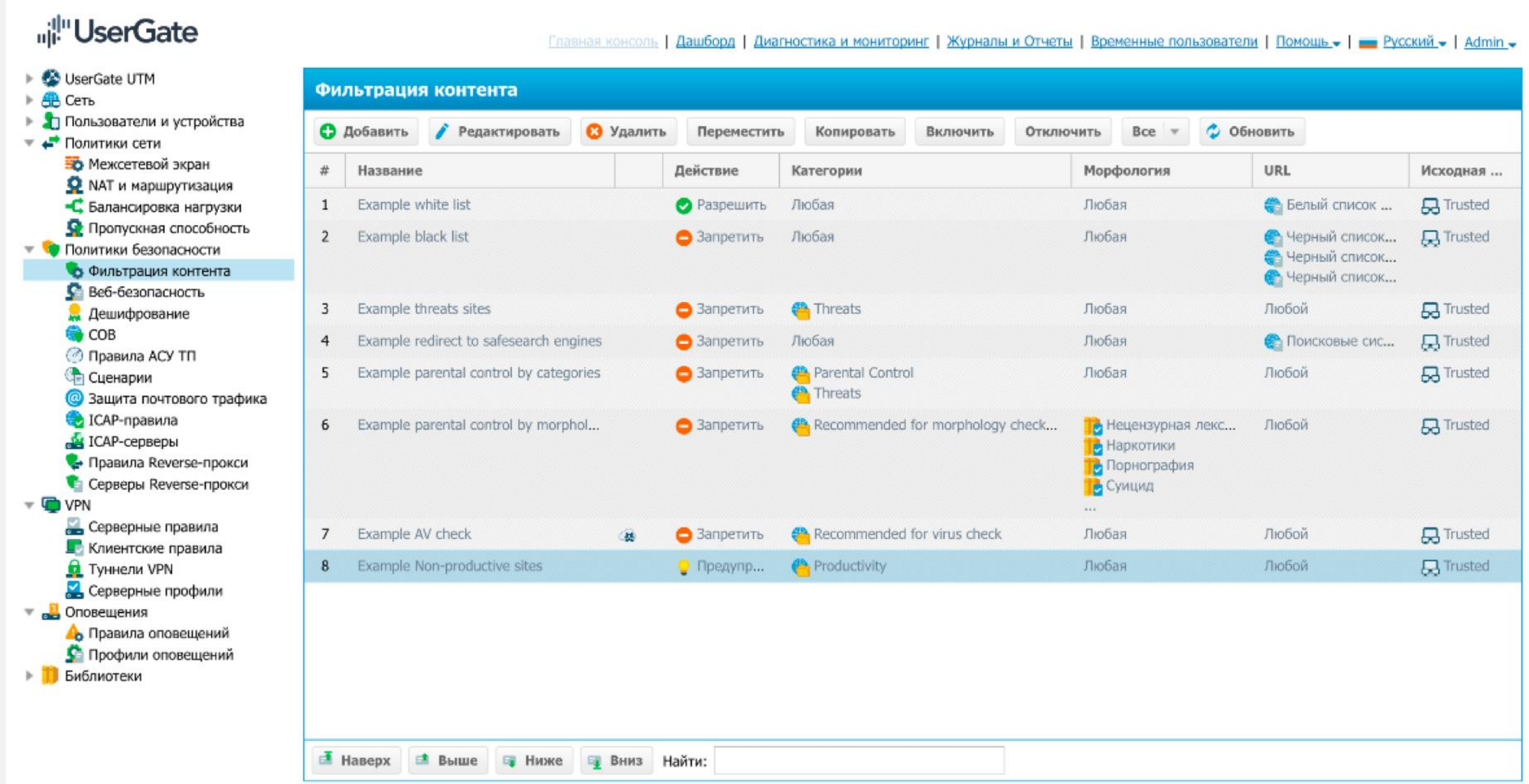
СОВ - Система обнаружения и предотвращения вторжений (IPS - Intrusion Prevention System)

Позволяет реагировать на атаки злоумышленников, использующих известные уязвимости, а также распознавать вредоносную активность внутри сети.

Администратор может создавать различные профили (наборы сигнатур, релевантных для защиты определенных сервисов) и задавать правила, определяющие действия для выбранного типа трафика (IP, ICMP, TCP, UDP), который будет проверяться в соответствии с назначенными профилями

Reverse Proxy - обратный прокси используется для безопасной публикации корпоративного портала и различных внутренних систем, таких как CRM, ERP, почта, а также для обеспечения доступа к определенным файлам, находящимся на внутренних серверах.

SSL VPN – позволяет сотрудникам получить безопасный доступ к корпоративным ресурсам через любой браузер, предоставляя удобство использования SSO для опубликованных сервисов, поддерживающих авторизацию по Kerberos, NTLM, SAML


UserGate
Главная консоль | Дашборд | Диагностика и мониторинг | Журналы и Отчеты | Временные пользователи | Помощь | Русский | Admin
UserGate UTM
Сеть
Пользователи и устройства
Политики сети
Межсетевой экран
NAT и маршрутизация
Балансировка нагрузки
Пропускная способность
Политики безопасности
Фильтрация контента
Веб-безопасность
Дешифрование
СОВ
Правила АСУ ТП
Сценарии
Защита почтового трафика
ICAP-правила
ICAP-серверы
Правила Reverse-прокси
Серверы Reverse-прокси
VPN
Серверные правила
Клиентские правила
Туннели VPN
Серверные профили
Оповещения
Правила оповещений
Профили оповещений
Библиотеки
Фильтрация контента
Добавить
Редактировать
Удалить
Переместить
Копировать
Включить
Отключить
Все
Обновить
| Название | Действие | Категории | Морфология | URL | Исходная ...
1 | Example white list | Разрешить | Любая | Любая | Белый список ... | Trusted
2 | Example black list | Запретить | Любая | Любая | Черный список... Черный список... Черный список... | Trusted
3 | Example threats sites | Запретить | Threats | Любая | Любой | Trusted
4 | Example redirect to safesearch engines | Запретить | Любая | Любая | Поисковые сис... | Trusted
5 | Example parental control by categories | Запретить | Parental Control Threats | Любая | Любой | Trusted
6 | Example parental control by morphol... | Запретить | Recommended for morphology check... | Нецензурная лекс... Наркотики Порнография Суицид ... | Любой | Trusted
7 | Example AV check | Запретить | Recommended for virus check | Любая | Любой | Trusted
8 | Example Non-productive sites | Предупр... | Productivity | Любая | Любой | Trusted
Наверх
Выше
Ниже
Вниз
Найти:

UserGate лицензируются по количеству одновременно использующих его пользователей, точнее IP- адресов, с которых подключаются устройства пользователей.

Дополнительно ежегодно лицензируются следующие модули:

- **Security Updates.** Включает обновления ПО UserGate, обновления операционной системы, баз сигнатур вторжений и известных приложений (L7), а также техническую поддержку.
- **Advanced Threat Protection.** Включает подписку на использование баз DNS-фильтрации, морфологических словарей и антивируса UserGate, определяющего репутацию файлов.
- **Heuristic Antivirus.** Включает подписку на антивирус с эвристическим анализом.

UserGate лицензируются по количеству одновременно использующих его пользователей, точнее IP- адресов, с которых подключаются устройства пользователей.

Дополнительно ежегодно лицензируются следующие модули:

- В базовую лицензию включена годовая подписка на Security Updates
- Действует скидка при единовременном приобретении дополнительных модулей на несколько лет
- Продление дополнительных модулей возможно только при активной подписке на модуль Security Updates

FORCEPOINT POWERED BY Raytheon

FORTINET

STONESOFT

Barracuda

KerioControl

BlueCoat

Microsoft Forefront

ПЛАТФОРМА UserGate

Платформа UserGate обладает всеми функциями межсетевого экрана нового поколения и не уступает мировым лидерам.

Платформа UserGate – это:

- Межсетевой экран нового поколения
- Обеспечение безопасности на уровне приложений (L7)
- Система обнаружения вторжений
- Поведенческий анализ потенциальных угроз
- Автоматическая реакция на неизвестные угрозы
- Применение гранулярных политик к пользователям
- Разбор защищенных протоколов (SSL)
- Глубокий анализ содержимого, загружаемого из интернета (DCI)

Зарубежные решения

Check Point, Cisco, Dell SonicWALL, Fortinet, Juniper Networks, McAfee, Sophos, WatchGuard, Barracuda Networks, Palo Alto Networks, StoneSoft

Зарубежные решения на данный момент серьезно доминируют на российском рынке во всех сферах, кроме тех, где требуются сертификаты ФСБ

Российские альтернативы

Инфотекс, Код Безопасности, Alltel

Отечественные решения серьезно уступают в плане функциональности и производительности. Единственные их применения – это использование для работы с гостайной и организация VPN-соединений с ГОСТ-шифрованием

Недостатки других решений

- Высокая цена продления и поддержки/штрафы при несвоевременном продлении
- Вероятность внезапного прекращения поставки и поддержки
- Платформа, основанная на устаревших решениях
- Ограниченная поддержка русского языка
- Невозможность соответствия законодательства РФ
- Невозможность организации бесплатного пилота.

Преимущества UserGate

- ✓ Является единственным российским решением данного класса, имеющим признание за рубежом (состоит в пятерке лучших UTM-решений года по версии американского SC-Magazine)
- ✓ Работа решения основана на самой современной платформе, разработанной для телеком-проектов
- ✓ Адаптирован ко всем требованиям законодательства РФ
- ✓ Прямой контакт с компанией-разработчиком, возможность влияния на планы развития
- ✓ Возможность организации бесплатного пилота

СЕРТИФИКАТ ФСТЭК России № 3905

Данный уровень сертификации дает возможность использования решения в составе автоматизированных систем до класса защищенности 1Г, информационных системах персональных данных (ИСПДн) и государственных информационных системах (ГИС) до 1 класса (уровня) защищенности включительно, т. е. не обрабатывающих гостайну. Решение полностью удовлетворяют требованиям 17 и 21 приказов ФСТЭК России для обработки персональных данных 1-4 категорий.

СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 3905

Внесен в государственный реестр системы сертификации
средств защиты информации по требованиям безопасности информации
26 марта 2018 г.

Выдан: 26 марта 2018 г. Переоформлен: 25 мая 2020 г.
Действителен до: 26 марта 2021 г.

Настоящий сертификат удостоверяет, что **изделие «Универсальный шлюз безопасности «UserGate UTM»**, разработанное и производимое ООО «Юзергейт», является системой обнаружения вторжений и межсетевым экраном, соответствует требованиям по безопасности информации, установленным в документах «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2018) - по 4 уровню доверия, «Требования к межсетевым экранам» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа А четвертого класса защиты. ИТ.МЭ.А4.ПЗ» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа Б четвертого класса защиты. ИТ.МЭ.Б4.ПЗ» (ФСТЭК России, 2016), «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011), «Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ» (ФСТЭК России, 2012) при выполнении указаний по эксплуатации, приведенных в формуляре 643.95486689.UTM-01 30.

Сертификат выдан на основании технического заключения от 07.02.2018, оформленного по результатам сертификационных испытаний испытательной лабораторией АО «НПО «Эшелон» (аттестат аккредитации от 18.04.2017 № СЗИ RU.0001.01БИ00.Б018), экспертного заключения от 15.02.2018, оформленного органом по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 05.05.2016 № СЗИ RU.0001.01БИ00.А002), и технического заключения от 24.04.2020, оформленного по результатам испытаний испытательной лабораторией АО «НПО «Эшелон».

Заявитель: ООО «Юзергейт»
Адрес: 630090, г. Новосибирск, ул. Николаева, д. 11, оф. 602
Телефон: (383) 286-2913

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

В.Лютиков

Применение сертифицированной продукции, указанной в настоящем сертификате соответствия, на объектах (объектах информатизации) разрешается при наличии сведений о ней в государственном реестре средств защиты информации по требованиям безопасности информации

Фильтрация HTTPs?

Решение UserGate позволяет производить инспекцию, дешифрацию SSL-трафика, также осуществляет подмену сертификатов (MitM), соответственно весь зашифрованный SSL трафик возможно анализировать также как и не шифрованный. (включая TLS 1.3)

Российская компания?

ООО «Юзергейт» Российская компания, не имеющая иностранных инвестиций, основанная в 2001 году в г. Новосибирске

Реестр российского ПО?

Решение UserGate включено в Единый Реестр Российского ПО.

Рег. номер ПО:1194 в реестре Минкомсвязи

ДЕПАРТАМЕНТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ХАНТЫ-МАНСИЙСКОГО АВТОНОМНОГО ОКРУГА — ЮГРЫ

Задачи:

- Замена зарубежного решения
- Обеспечение функций прокси-сервера
- Интернет-фильтрация

Решение:

- Виртуальная платформа UserGate
- Модуль ATP (расширенная защита от угроз нового поколения)

«Мы убедились, что UserGate является надежным, удобным и функциональным решением, ни в чем не уступающим известным нам зарубежным решениям», – заявил директор Бюджетного учреждения «Окружной центр ИКТ» Степан Перевертайло.

ГРУППА КОМПАНИЙ ФОСАГРО

В группе компаний Фосагро UserGate используется для доступа в сеть.
На всех доменных ПК используется SSO и авторизация Kerberos, в основном офисе более 2000 пользователей. Для авторизации при подключению к публичному гостевому WiFi используется Captive Portal. Основная задача, решаемая UserGate состоит в сложной фильтрации http/https трафика по определённым группам пользователей, запрет интернет ресурсов по категориям, антивирусная проверка трафика на уровне шлюза, фильтрация по спискам. Все эти меры обеспечивают эффективное использование интернет-ресурсов сотрудниками компании.

По просьбе заказчика была реализована возможность отправлять весь входящий в UserGate трафик по протоколу ICAP на сервер с DLP (SearchInform) для дальнейшего анализа. Также была расширена информация передаваемая по ICAP на DLP сервер, добавлена информация о неавторизованных пользователях – по IP и MAC-адресу.

ИСПОЛЬЗОВАНИЕ UserGate ПРИ ПРОВЕДЕНИИ ВСЕМИРНОЙ ЗИМНЕЙ УНИВЕРСИАДЫ

29TH WINTER UNIVERSIADE
KRASNOYARSK 2019

Задачи:

- Корпоративный межсетевой экран
- Обеспечение функций прокси-сервера
- Защита от угроз нового поколения
- Безопасная публикация через обратный прокси

Решение:

- Аппаратные платформы UserGate F8000 – 2 шт, UserGate E1000 – 4 шт с модулем ATP и UserGate D500 – 4 шт.

ГЛАВНОЕ УПРАВЛЕНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СВЯЗИ ОМСКОЙ ОБЛАСТИ

Задачи:

- Корпоративный межсетевой экран
- Обеспечение функций прокси-сервера
- Защита электронной почты

Решение:

- Аппаратные платформы UserGate с модулем Mail Security до 3000 пользователей

«Нам понравилось, что мы получили не просто решение с правильными сертификатами, но и при этом обладающее сильной функциональностью и надежностью», – заявил Оболенский Денис Александрович, начальник отдела информационной безопасности Главного управления информационных технологий и связи Омской области

РОССИЙСКАЯ САМОЛЕТОСТРОИТЕЛЬНАЯ КОРПОРАЦИЯ «МиГ»

Задачи:

- Замена зарубежного решения
- Обеспечение функций прокси-сервера
- Интернет-фильтрация
- Интеграция с DLP-решением

Решение:

- Виртуальная платформа UserGate с модулем ATP

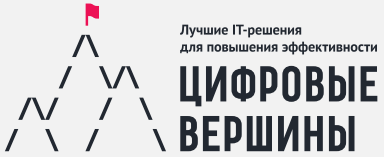
Мы испытываем исключительно положительные впечатления от нового решения UserGate», – заявил Александр Викторович Руденко, Заместитель начальника управления внедрения и сопровождения ИТ инфраструктуры и сервисов АО «РСК «МиГ»

ИТ-ИНФРАСТРУКТУРА ПАО «МРСК СИБИРИ»

Инженеры UserGate совместно с инженерами партнера и инженерами ПАО «МРСК Сибири» в сжатые сроки произвели конфигурирование оборудования и обеспечили полноценную работу ИТ-инфраструктуры предприятия. Среди прочего была выполнена настройка правил ограничения доступа в интернет, правил контроля приложений, правил межсетевых экранов на границах сети интернет, смежных организаций и серверного сегмента. Помимо этого, была реализована защита web-ресурсов, безопасная публикация через обратный прокси и настроена Single Sign-On авторизация для опубликованных web-сервисов.

В подтверждение высокого качества UserGate стал финалистом конкурса SC Awards 2014 американского журнала SC Magazine наравне с WebSense, Barracuda, Fortinet и ClearSwift и победителем SC Awards 2015 SC Magazine Awards Europe британского издания SC Magazine, опередив в финале Trustwave, Websense и Barracuda Networks. В феврале 2017 года UserGate вошел в пятерку лучших UTM-решений года.

В декабре 2018 Программно-аппаратное и виртуальное решение UserGate было удостоено премии «Цифровые вершины» в номинации «Лучшее решение для повышения информационной безопасности»



UserGate

sales@usergate.ru | usergate.ru