UserGate

Безопасность для сетей любого размера

Чернов Иван
Партнерский отдел компании UserGate
e-mail: ichernov@usergate.com
M: +7(983)129-13-06

О компании

Наш офис разработки находится в Технопарке Новосибирского Академгородка, в месте, где тысячи талантливых разработчиков, инженеров, ученых занимаются производством высокотехнологичных продуктов.

В апреле 2019 года открылось представительство в Москве.

Что сейчас на рынке информационной безопасности?

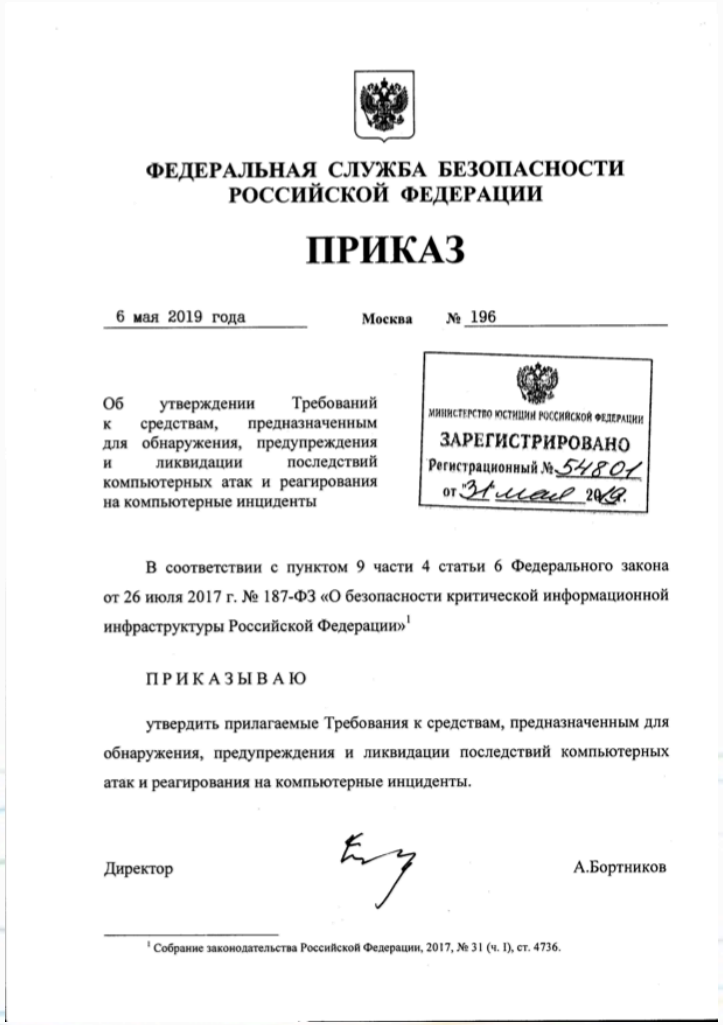
Информационное сообщение ФСТЭК России от 29 марта 2019 г. N 240/24/1525

https://fstec.ru/normotvorcheskaya/informatsionnye-i-analiticheskie-materialy/1812-informatsionnoe-soobshchenie-fstek-rossii-ot-29-marta-2019-g-n-240-24-1525

О ТРЕБОВАНИЯХ ПО БЕЗОПАСНОСТИ ИНФОРМАЦИИ, УСТАНАВЛИВАЮЩИХ УРОВНИ ДОВЕРИЯ К СРЕДСТВАМ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ И СРЕДСТВАМ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

UserGate

Приказ №196
Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

6 мая 2019 года Москва № 196

Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 54801
от 31 мая 2019

В соответствии с пунктом 9 части 4 статьи 6 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»[1]

ПРИКАЗЫВАЮ

утвердить прилагаемые Требования к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.

Директор А.Бортников

[1] Собрание законодательства Российской Федерации, 2017, № 31 (ч. I), ст. 4736.

Реальные угрозы

- Усложнение атак
- Расширение сфер деятельности злоумышленников
- Развитие технологий

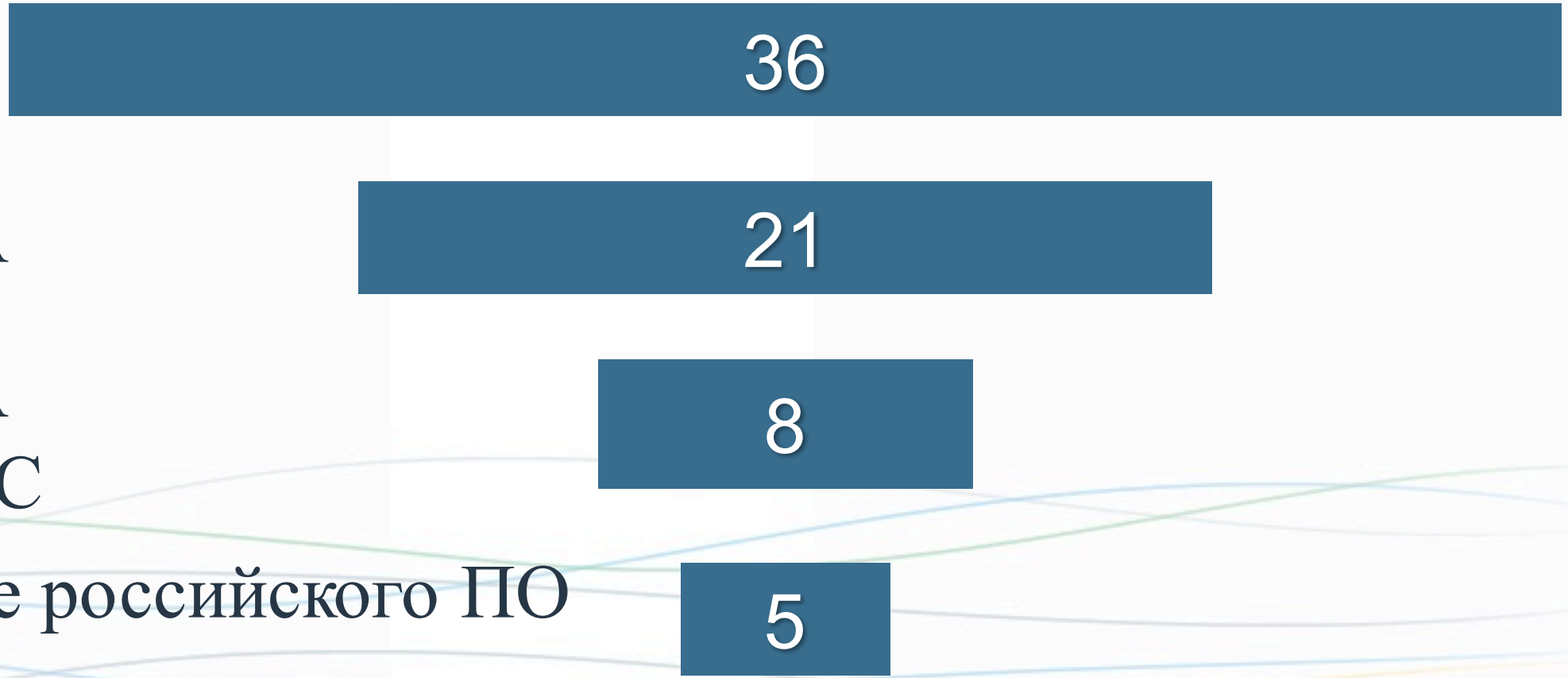
Требования законодательства

- 152-ФЗ – Персональные данные
- 187-ФЗ – КИИ
- 139-ФЗ и 436-ФЗ – Защита детей от нежелательной информации

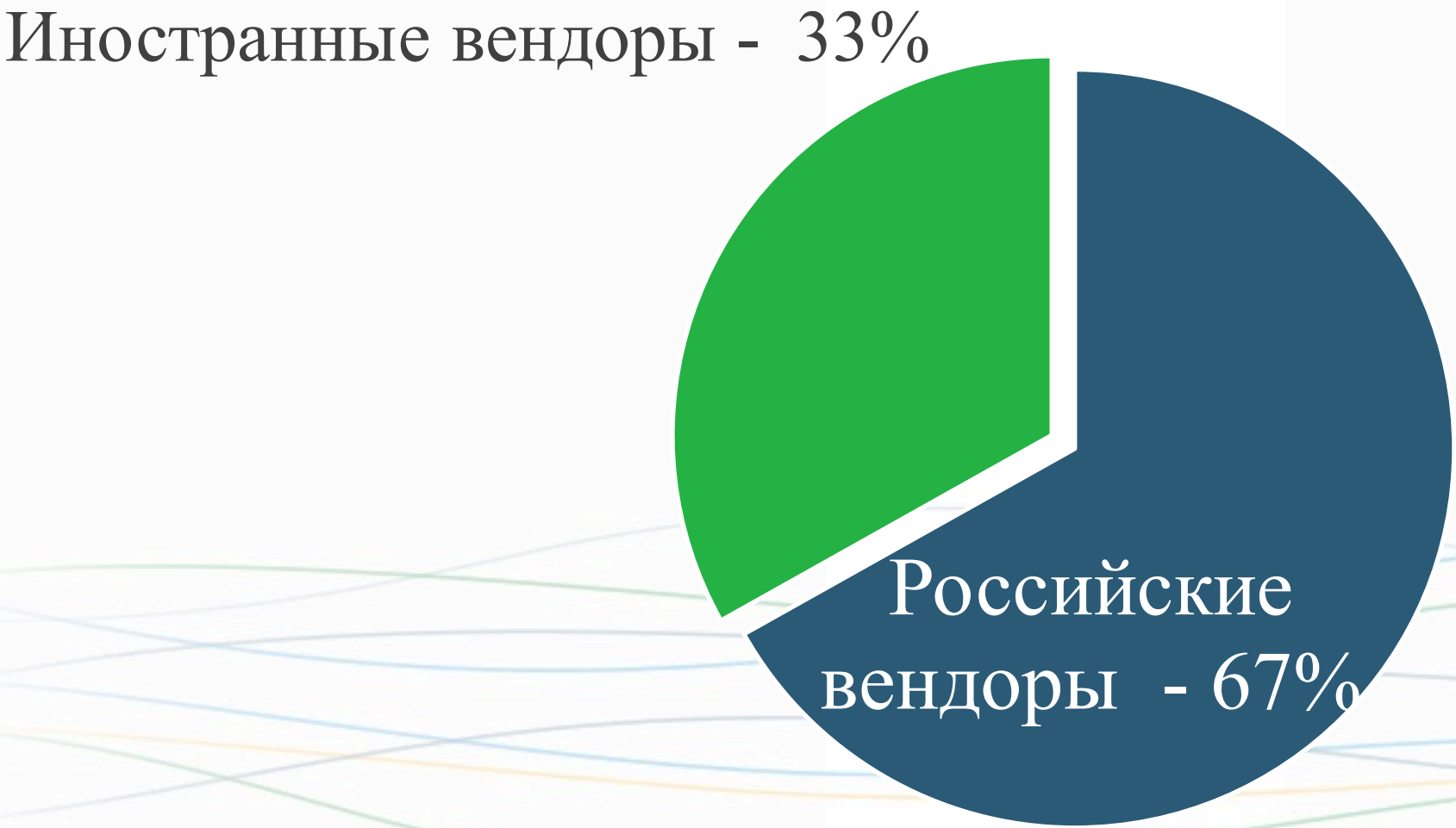
Растет запрос на защиту

Ситуация на рынке

Сертификатов, выданных на серию в реестре ФСТЭК:



Соотношение сертификатов ФСТЭК выданных на серию, с профилем защиты ИТ.МЭ

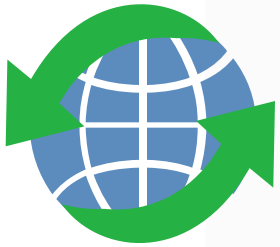


Что необходимо для защиты от угроз?

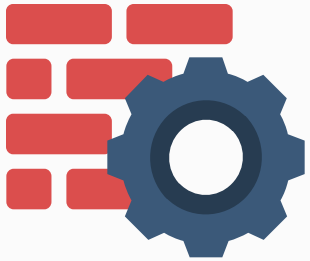
UserGate

Что необходимо для защиты от угроз?

Безопасная публикация ресурсов и сервисов



Анализ и предотвращение новых угроз (SOAR)



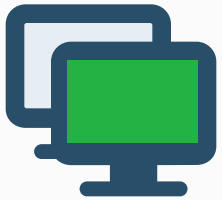
Межсетевой экран NGFW

Интернет фильтрация

Система обнаружения и предотвращения вторжений

Безопасная публикация сервисов

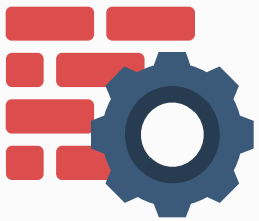
Reverse Proxy - обратный прокси используется для безопасной публикации корпоративного портала и различных внутренних систем, таких как CRM, ERP, почта, а также для обеспечения доступа к определенным файлам, находящимся на внутренних серверах.



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

Next Generation Firewall

Межсетевой экран нового поколения
(NGFW - Next Generation Firewall)
должен обеспечивать:



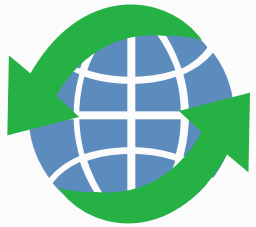
- ✓ Высокую скорость обработки трафика
- ✓ Применением гибких политик к пользователям
- ✓ Контроль приложений на L7 уровне по всем портам
- ✓ Интернет-фильтрацию, инспекцию SSL-трафика
- ✓ Идентификацию пользователей
- ✓ Антивирусную защиту

Система предотвращения вторжений

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

Анализ угроз (Проактивная защита)



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.

Сценарий является дополнительным условием в правилах межсетевого экрана и пропускной способности, позволяя администратору настроить реакцию решения на возникновение определенных событий для обеспечения проактивной защиты.

Безопасность почты

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.

Интернет-фильтрация

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.

О решениях на платформе UserGate

UserGate

Другие функции

Поддержка АСУ ТП (SCADA)

Контроль доступа в интернет

Гостевой портал

Контроль приложений на уровне L7

Безопасная публикация ресурсов и сервисов

Идентификация пользователей

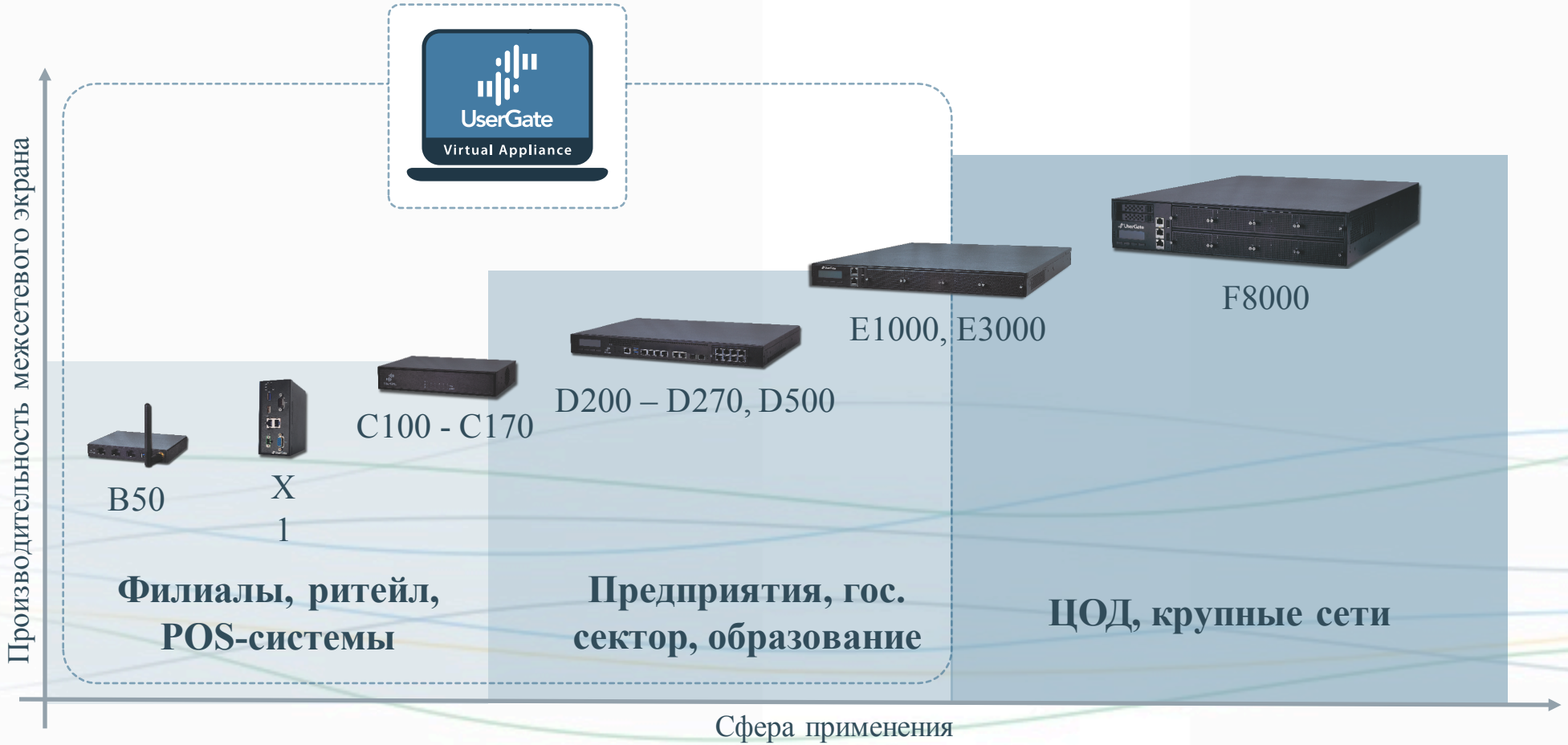
Дешифрование SSL

Антивирусная защита

Контроль мобильных устройств, поддержка концепции BYOD

О платформе UserGate

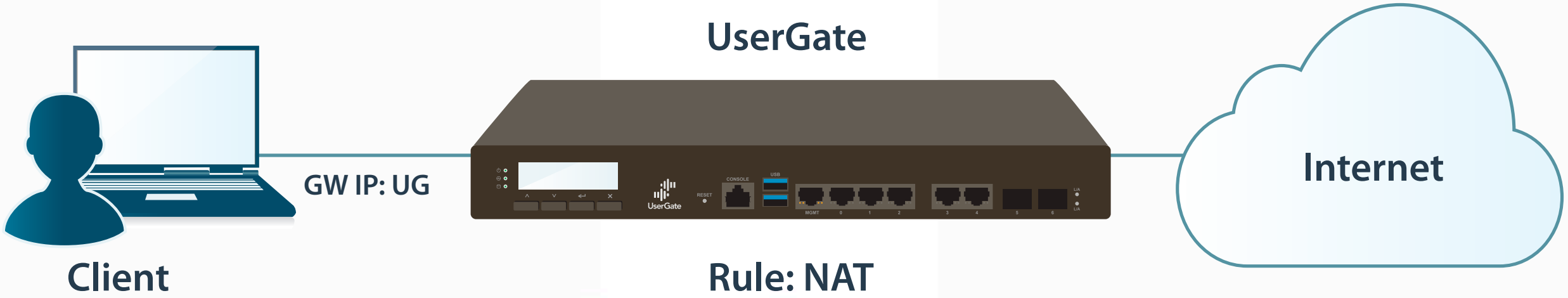
Работа решений линейки UserGate основана на одноименной платформе, доступной в виде виртуального решения (готового образа для VMware, Hyper-V и прочих систем виртуализации) или в виде appliance, то есть программно-аппаратного комплекса.



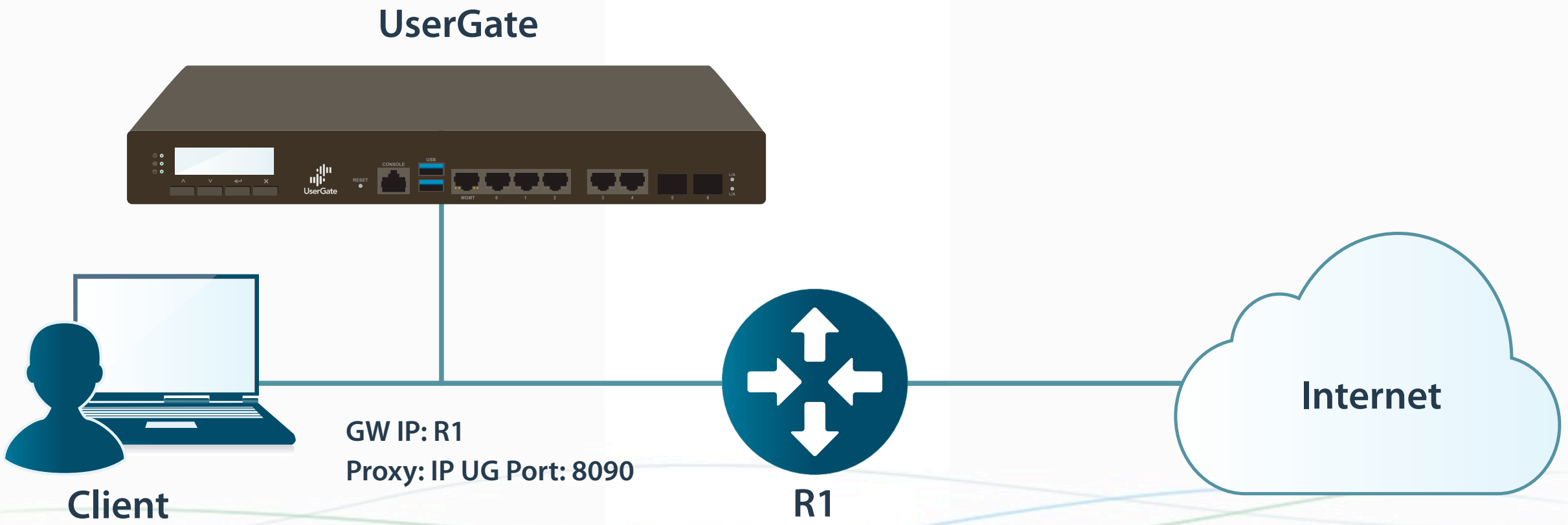
vmware
VirtualBox
openstack
Hyper-V
Xen
KVM
Microsoft Azure
amazon web services

Сценарии применения

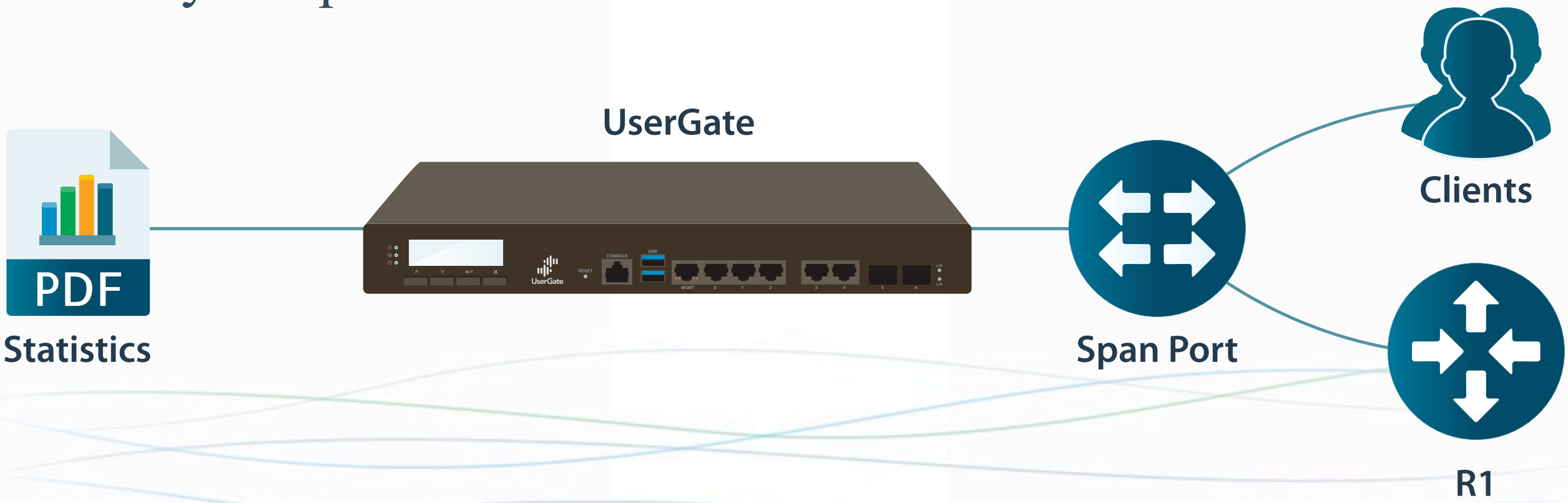
Шлюз по умолчанию



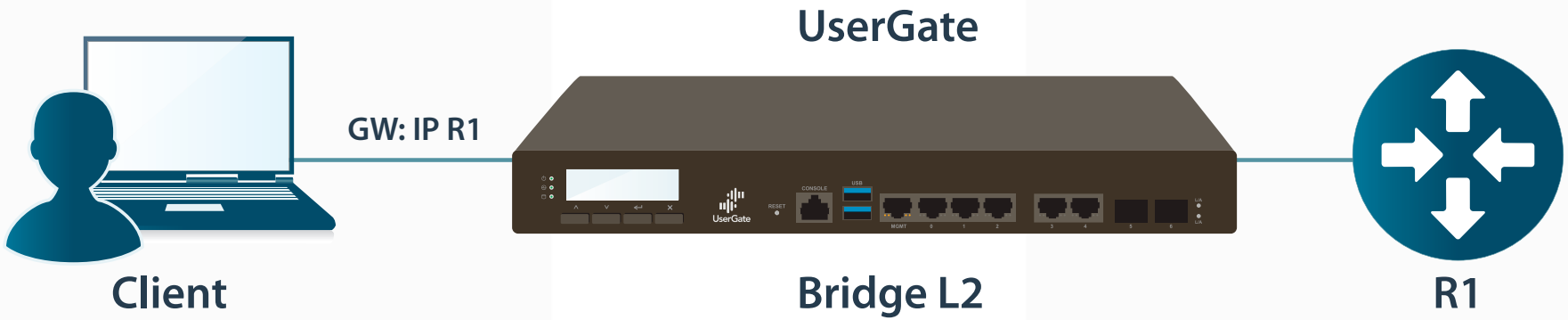
Прокси сервер



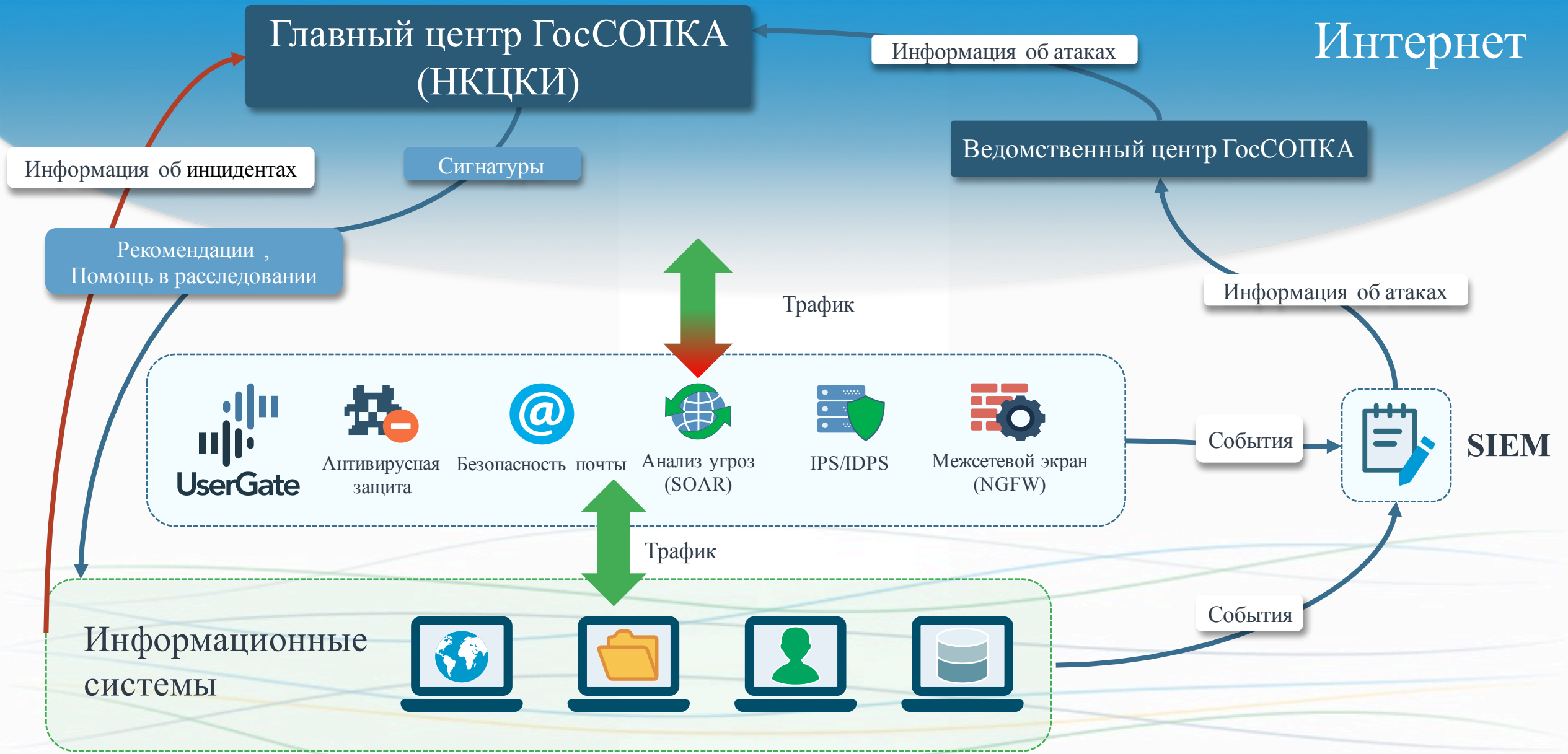
Работа с зеркальным трафиком со SPAN порта коммутатора



Transparent bridge L2



Как это работает?



UserGate

Импортозамещение

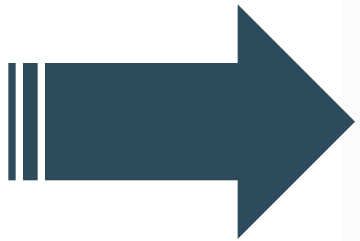
Импортозамещение

Платформа UserGate обладает всеми функциями межсетевого экрана нового поколения и не уступает мировым лидерам, таким как Check Point, Fortinet, Palo Alto Networks

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)


FORCEPOINT
POWERED BY Raytheon
Microsoft
Forefront
Threat Management Gateway 2010
BlueCoat
FORTINET
Barracuda
STONESOFT
KerioControl



UserGate

Сертификат ФСТЭК

СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 3905

Выдан 26 марта 2018 г.
Действителен до 26 марта 2021 г.

Настоящий сертификат удостоверяет, что изделие «Универсальный шлюз безопасности «UserGate UTM», разработанное и производимое ООО «СЛ Девелопмент», является системой обнаружения вторжений и межсетевым экраном, соответствует требованиям документов «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) и «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 643.95486589.UTM-0130.

Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией АО «НПО «Эшелон» (аттестат аккредитации от 18.04.2017 № СЗИ RU.0001.01БИ00.БО18) - технические заключения от 07.02.2018, экспертного заключения от 15.02.2018 органа по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 05.05.2016 № СЗИ RU.0001.01БИ00.А002).

Заявитель: ООО «СЛ Девелопмент» (ИНН 5408243746)
Адрес: 630090, г. Новосибирск, ул. Николаева, д. 11, оф. 602,
Телефон: (383) 286-2913

Контроль маркирования знаками соответствия сертифицированной продукции и инспекционный контроль её соответствия требованиям документов, указанных в настоящем сертификате, осуществляются испытательной лабораторией АО «НПО «Эшелон».

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

В.Лютиков

Настоящий сертификат внесен в Государственный реестр сертифицированных средств защиты информации
26 марта 2018 г.

Решение UserGate прошло сертификацию **ФСТЭК по 4 классу документа «Требования к межсетевым экранам (ФСТЭК, 2016)»**, **профили защиты А и Б**, а также по **4 классу документа «Требования к системам обнаружения вторжений (ФСТЭК, 2011)»**.

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 для обработки персональных данных 1-4 категорий.

Сертификат ФСТЭК №3905 от 26 марта 2018 г.

Нас выбирают

Безопасность инфраструктуры ПАО “МРСК Сибири

Использование UserGate при проведении Всемирной зимней универсиады

МРСК СИБИРИ

KRASNOYARSK 2019
29TH WINTER UNIVERSIADE

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.

Безопасность в государственных структурах

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.

Безопасность в авиационной промышленности

Российская самолетостроительная корпорация «МиГ»

Задачи:

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

Решение:

- Виртуальная платформа UserGate с модулем АТР

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».

Защита органов власти от интернет-угроз

Департамент информационных технологий Ханты-Мансийского автономного округа — Югры

Задачи:

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

Решение:

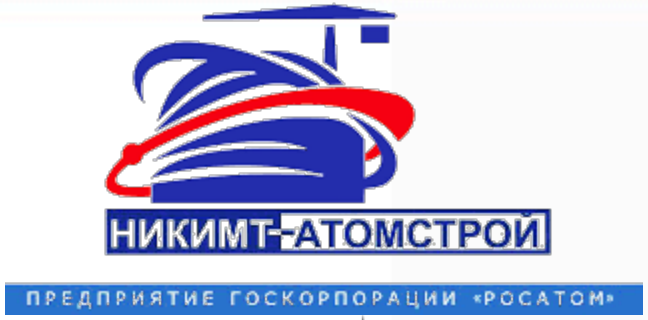
- Виртуальная платформа UserGate с модулем АТР до 2500 сессий.

«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.

UserGate

Нас выбирают:

ПРАВИТЕЛЬСТВО МОСКВЫ



UserGate

Нас выбирают:

Музеи Московского Кремля

Госкорпорация по ОрВД

ОГК-2

горки город

Царицыно
музей-заповедник

Транснефть

Газпром Межрегионгаз

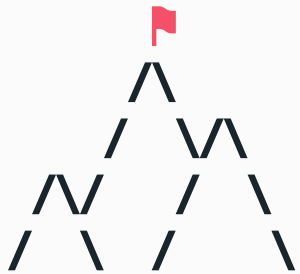
ФОСАГРО

lady & gentleman CITY

KFC

Сургутнефтегаз

Награды



Лучшие IT-решения
для повышения эффективности
ЦИФРОВЫЕ
ВЕРШИНЫ

В подтверждение высокого качества UserGate стал финалистом конкурса SC Awards 2014 американского журнала SC Magazine наравне с WebSense, Barracuda, 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 года UserGate стал лауреатом Российской премии "Цифровые вершины" в номинации "Лучшее решение для повышения информационной безопасности".

https://www.scmagazine.com/sc-awards-finalists-2017-round-six/article/572883

Спасибо за внимание

www.usergate.com | sales@usergate.com

UserGate

Безопасность для сетей любого размера

Чернов Иван
Партнерский отдел компании UserGate
e-mail: ichernov@usergate.com
M: +7(983)129-13-06