UserGate

UserGate SUMMA.

100% видимость трафика на базе собственных разработок

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

Дополнительные офисы: г. Москва, г. Санкт-Петербург, г. Хабаровск.

О компании UserGate

2001
запуск первой версии UserGate Proxy

2009
начало разработки первого российского NGFW UserGate

2010
создан внутренний стартап, в рамках которого началась разработка новой платформы

2012
UserGate – резидент Академпарка в Новосибирске

2015
UserGate – резидент Сколково

2016
выпуск нового UserGate как решения класса UTM

2018
создание экспертной лаборатории и начало разработки собственных аппаратных платформ

Сертификация новой платформы по требованиям ФСТЭК России

2019
открытие первого московского офиса UserGate

2020
открытие офиса UserGate в Хабаровске

начало экспансии UserGate с первым отечественным NGFW на рынке ИБ России

реализовано несколько тысяч проектов, в большинстве из которых замещены зарубежные аналоги

2021
выход на рынок экосистемы безопасности UserGate SUMMA

2022
открытие офиса в Санкт-Петербурге

Как USERGATE изменился В 2023 ГОДУ

- значительное увеличение штата **технической поддержи**;
- два офиса разработки + открытие офиса в РБ.;
- полноценный отдел pre-sale, состоящий из высококвалифицированных инженеров;
- отдел сервиса и качества (emergency team);
- технические лаборатории на базе подразделений UserGate;
- авторизованные учебные центры и новые учебные курсы+ академия UserGate ;
- тщательная проработка всех feature request
- выход версии релиз кандидат 7.1 (с SIEM, UG Client)

Ландшафт угроз 2024

Ландшафт угроз

- таргетированные атаки от проправительственных групировок;
- видим применение бот-сетей для организации DDOS-атак, как правило приуроченных к какому-то событию;
- высокую активность сохраняют «шифровальщики» (ransomware);
- скорость реакции на выходящие PoC очень высокая;
- наиболее популярными остаются веб-приложения и чаще эксплуатируют уязвимости имеющие PoC.

Требования регуляторов

Требования регуляторов

- 187-ФЗ от 26.07.2017
- 152-ФЗ от 27.07.2006
- Приказ ФСТЭК №21 от 18.02.2013
- Приказ ФСТЭК №17 от 11.02.2013
- 436-ФЗ от 29.12.2010
- Приказ Минздрава России №911н от 24.12.2018
- 114-ФЗ от 25.07.2002

Сертификат ФСТЭК России № 3905

Решение UserGate имеет действующий сертификат ФСТЭК России по 4 уровню доверия до 26.03.2026 г.

- **Требования к МЭ**
  - Профиль защиты МЭ типа А 4-го класса защиты
  - Профиль защиты МЭ типа Б 4-го класса защиты
  - Профиль защиты МЭ типа Д 4-го класса защиты
- **Требования к СОВ**
  - Профиль защиты СОВ уровня сети 4-го класса защиты

Уровень доверия 4:

- классы защиты СЗИ 4;
- ЗО КИИ 1 категории;
- ГИС 1 класса;
- АСУ ТП 1 класса;
- ИСПДн 1 уровня;
- ИСОП II класса.

Ожидания рынка

Ожидания рынка

- Снижение стоимости 1 Гб/с/руб (FPGA, производительность)
- Стабильность решения
- Сервис
- Зрелое сообщество
- Реальный кибербез
- Внятный road-map
- Функционал
- …

Функционал

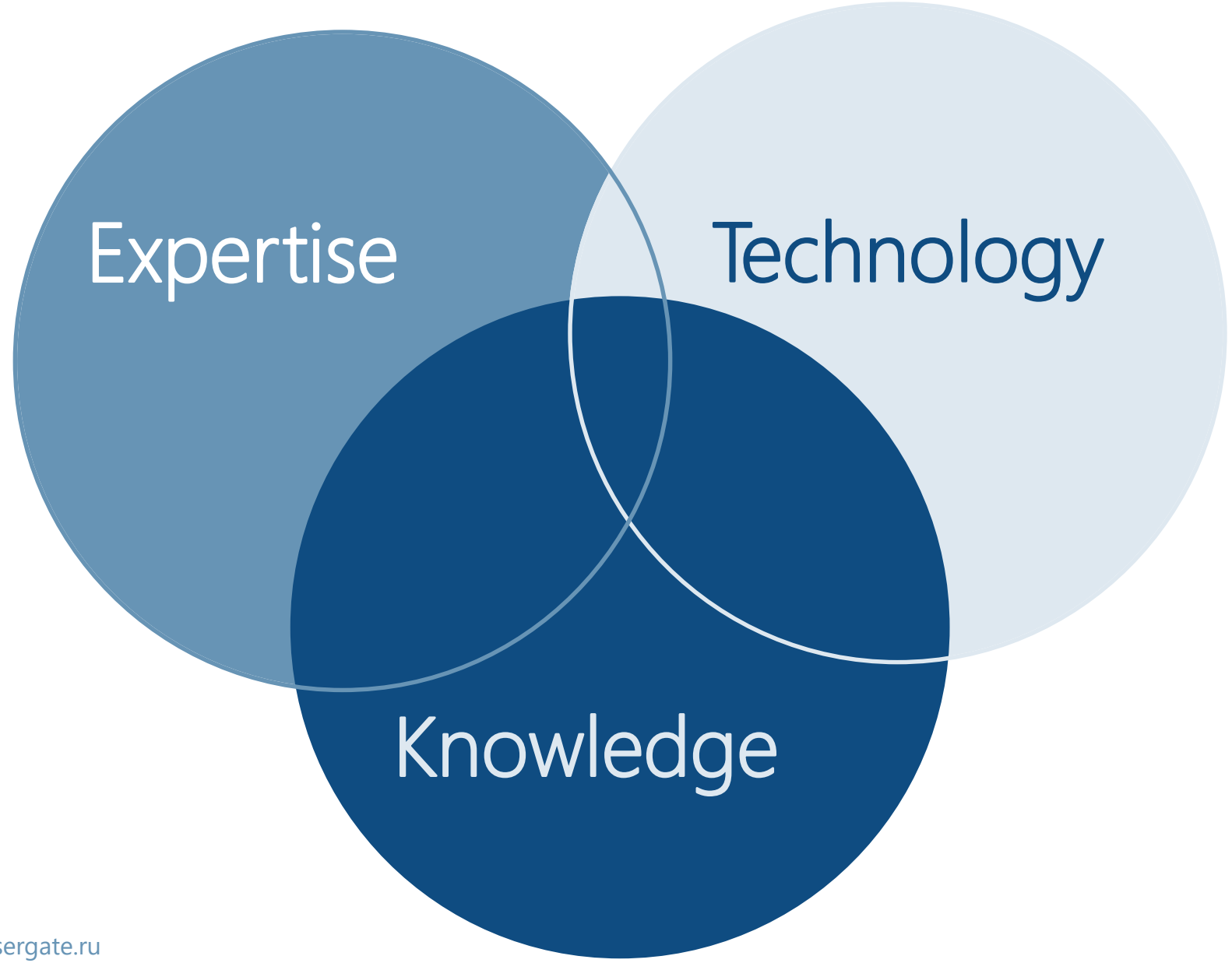
- VPN (ssl vpn)
- NAC, EDR
- Полноценный debug
- Полноценный Proxy
- Ssl-inspection с проверкой IDPS L7
- 10k-500k rules
- Максимальный стек сетевых технологий

Функционал

- Автоматизация процессов ИБ
- CLI
- VDOM
- UserID
- …

Волшебная кнопка

Волшебная кнопка



Expertise

Технологии бесполезны если нет экспертизы в решении

- Сигнатуры IDPS/L7
- Правила для WAF
- Правила корреляции для SIEM
- Наполнение базы IoC, a/virus, url, IP
- Анализ защищенности
- SOC

Knowledge

Academy UserGate

- Программа обучения на базе собственных курсов или курсов партнеров
- Тестирование инженеров

Pre-sales UserGate

- Лабораторные (pre-sales)
- Знания особенностей работы других вендоров

О технологиях

UserGate NGFW

Межсетевой экран следующего поколения

Next-Generation Firewall

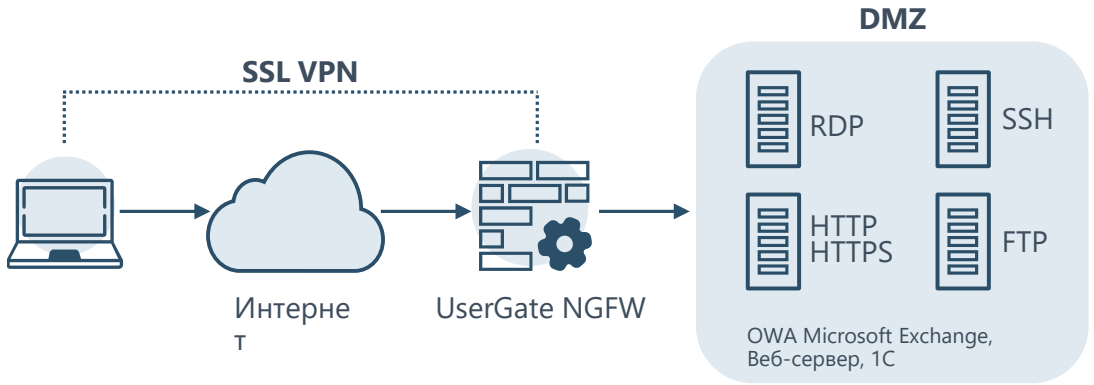
- Высокая скорость обработки трафика
- Идентификация пользователей
- Применение гибких политик к пользователям
- Контроль приложений на L7 уровне по всем портам
- Интернет-фильтрация, инспекция SSL-трафика с поддержкой TLS 1.3 и поддержкой TLS ГОСТ
- Инспекция SSH
- Защита от DoS-атак

Безопасный доступ

Next-Generation Firewall

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 (Веб-портал) – позволяет сотрудникам получить безопасный доступ к корпоративным приложениям через любой браузер, предоставляя удобство использования SSO для опубликованных сервисов, поддерживающих авторизацию по Kerberos, NTLM, SAML в том числе с поддержкой MFA.



Remote access VPN – для удаленного доступа клиентов.

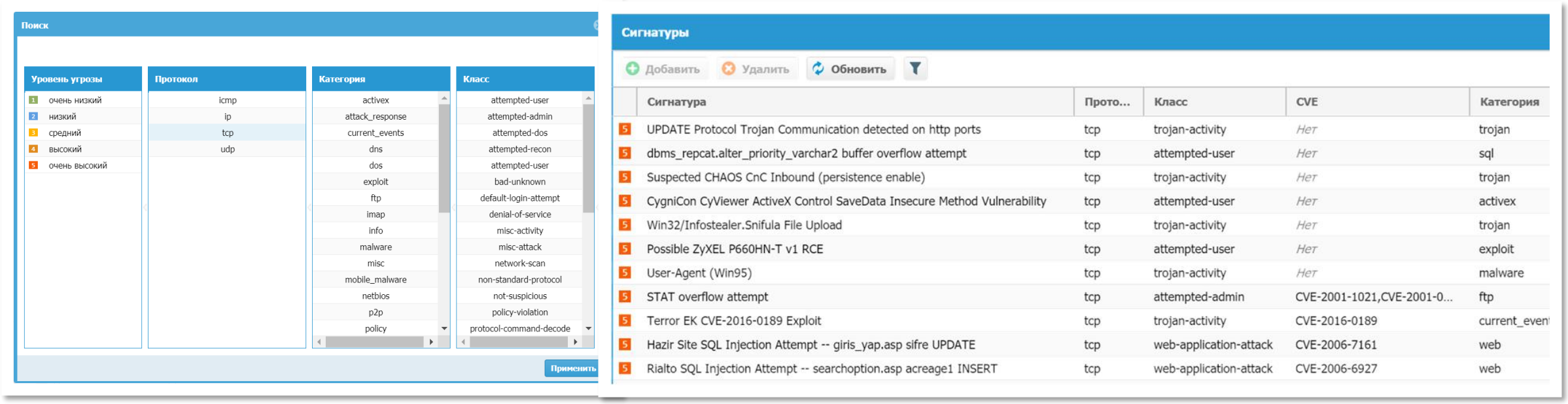
Site-to-Site VPN – для защищенного соединения офисов.

Для создания туннелей используется протокол Layer 2 Tunnelling Protocol (L2TP), а для защиты передаваемых данных – протокол IPSec. Поддерживается многофакторная авторизация пользователей при подключении к сервису VPN.

IDPS (COB)

Система обнаружения вторжений

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

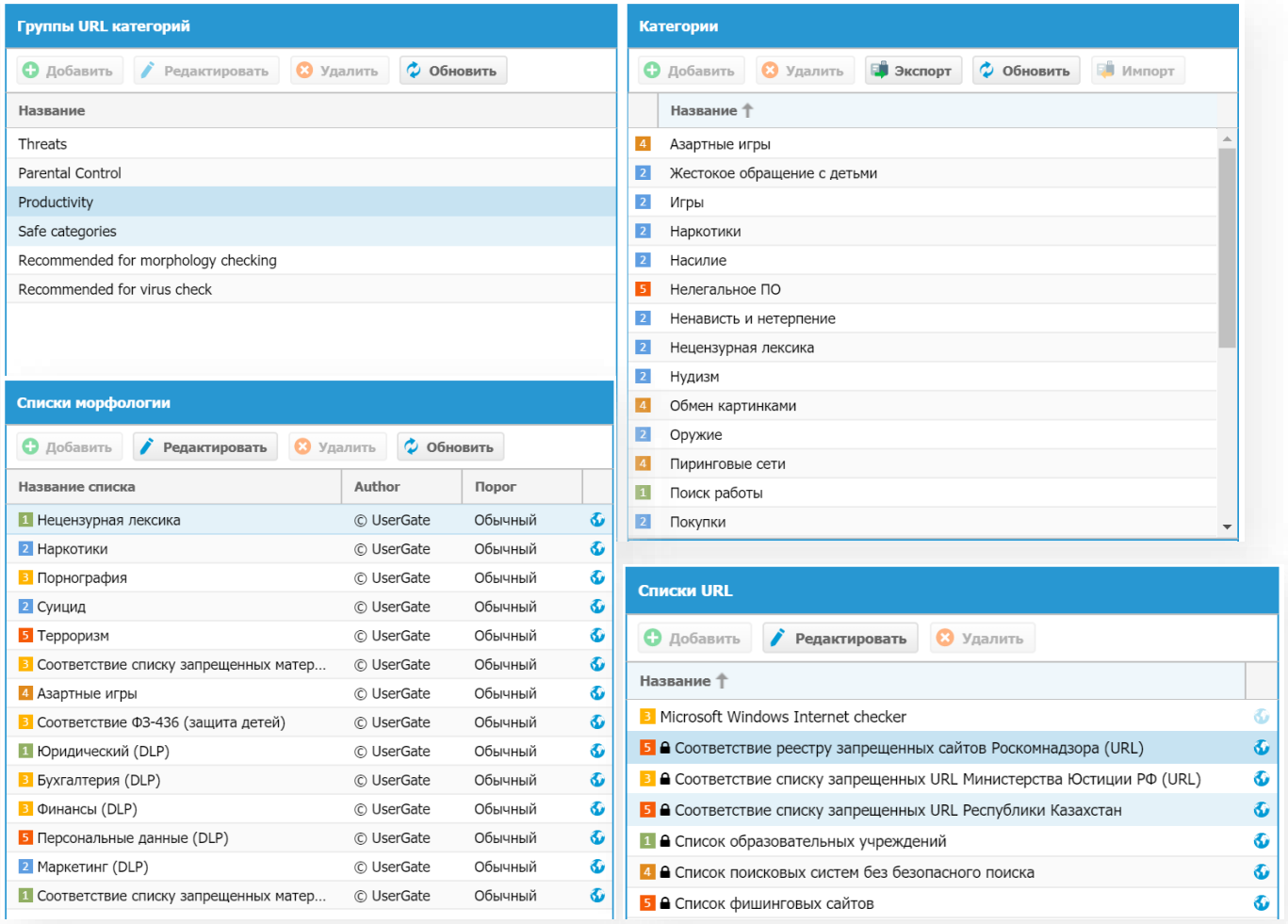


Контентная фильтрация

Механизмы фильтрации

- фильтрация по категориям;
- морфологический анализ;
- безопасный поиск;
- белые и черные списки;
- блокировка контекстной рекламы;
- запрет загрузки определенных видов файлов;
- антивирусная проверка трафика;
- интернет-фильтрация, инспекция SSL-трафика с поддержкой TLS 1.3 и TLS ГОСТ.

- крупнейшая база электронных ресурсов – более 600 миллионов сайтов;
- 80+ категорий;
- ежедневное обновление списка сайтов;
- повторная проверка уже внесенных ресурсов на предмет изменения контента и актуальности информации о категории.

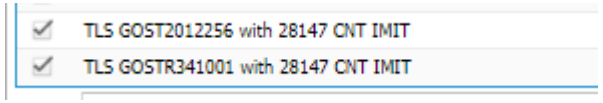


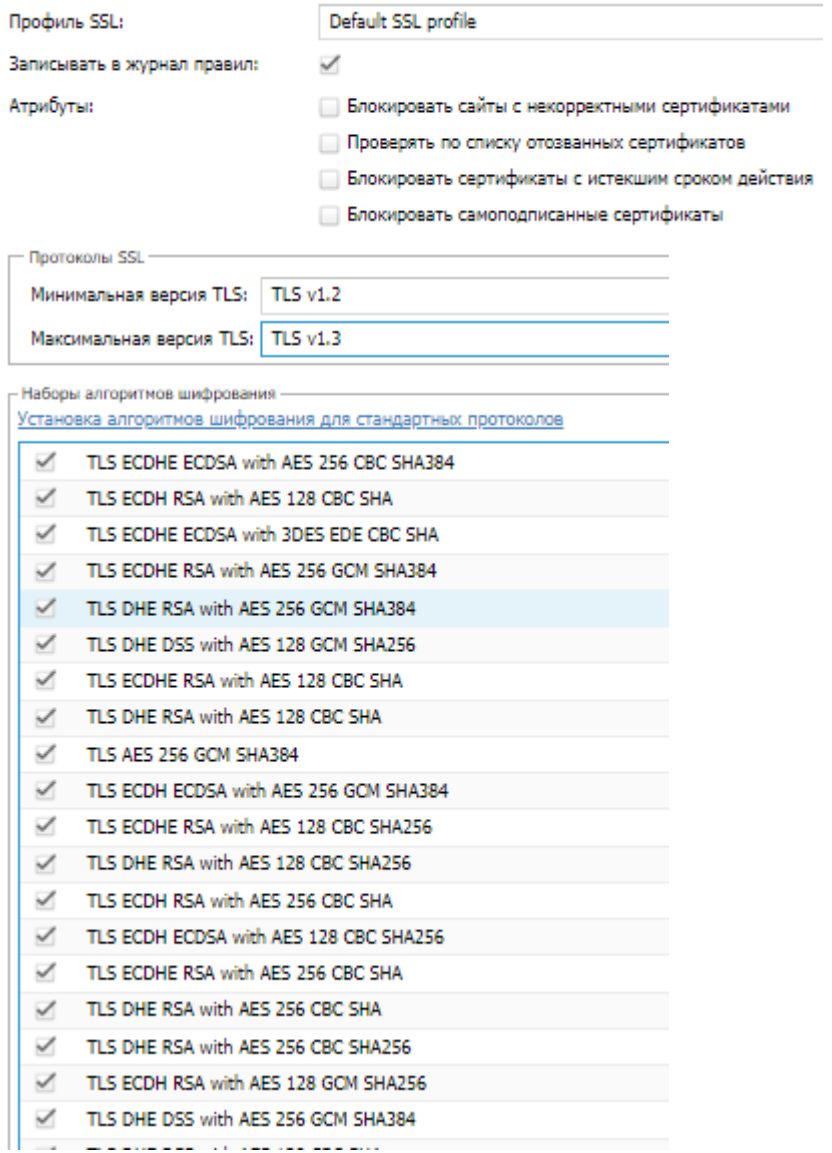
Про SSL-инспекцию

Про SSL-инспекцию

Обязательно:

- **Проверка всей цепочки сертификатов!!!**
- Выбор алгоритма шифрования (только strong)
- TLS 1.3, TLS ГОСТ
- Проверка движком IDPS



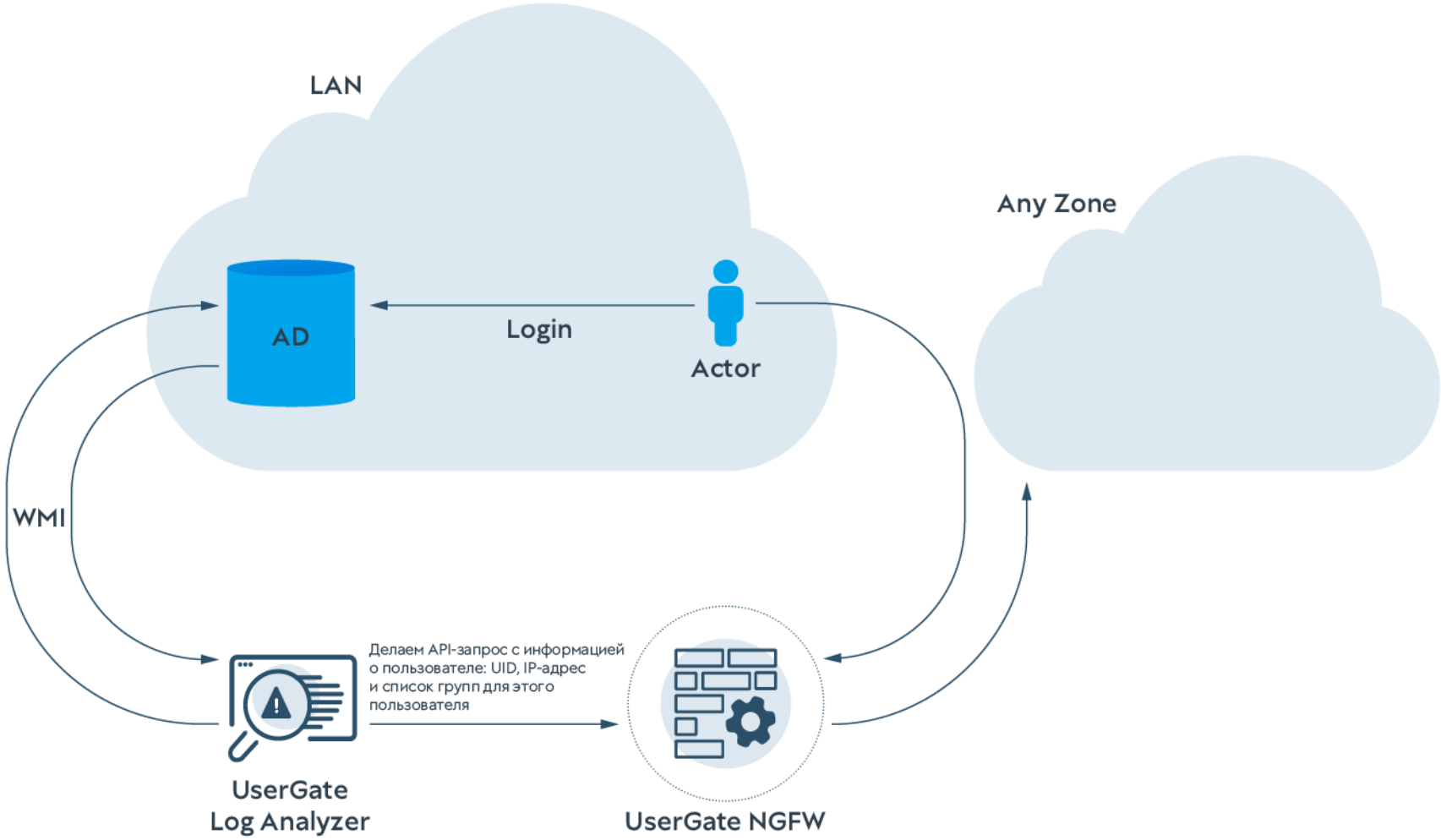


Новое в 7.1

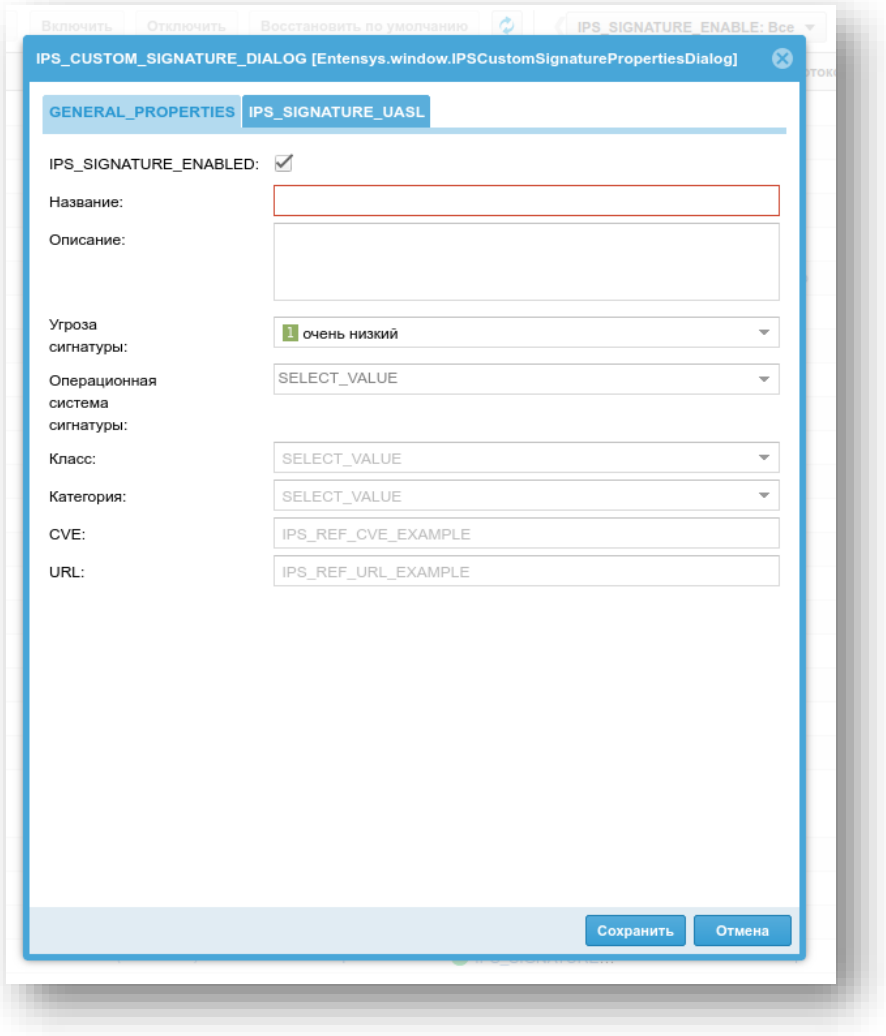
Новое в 7.1

- UserID
- Пользовательские сигнатуры IDPS&L7
- Новый движок IPSv3
- IKEv2
- Темная тема
- UserGate Client
- UserGate SIEM Light (MVP)

UserID

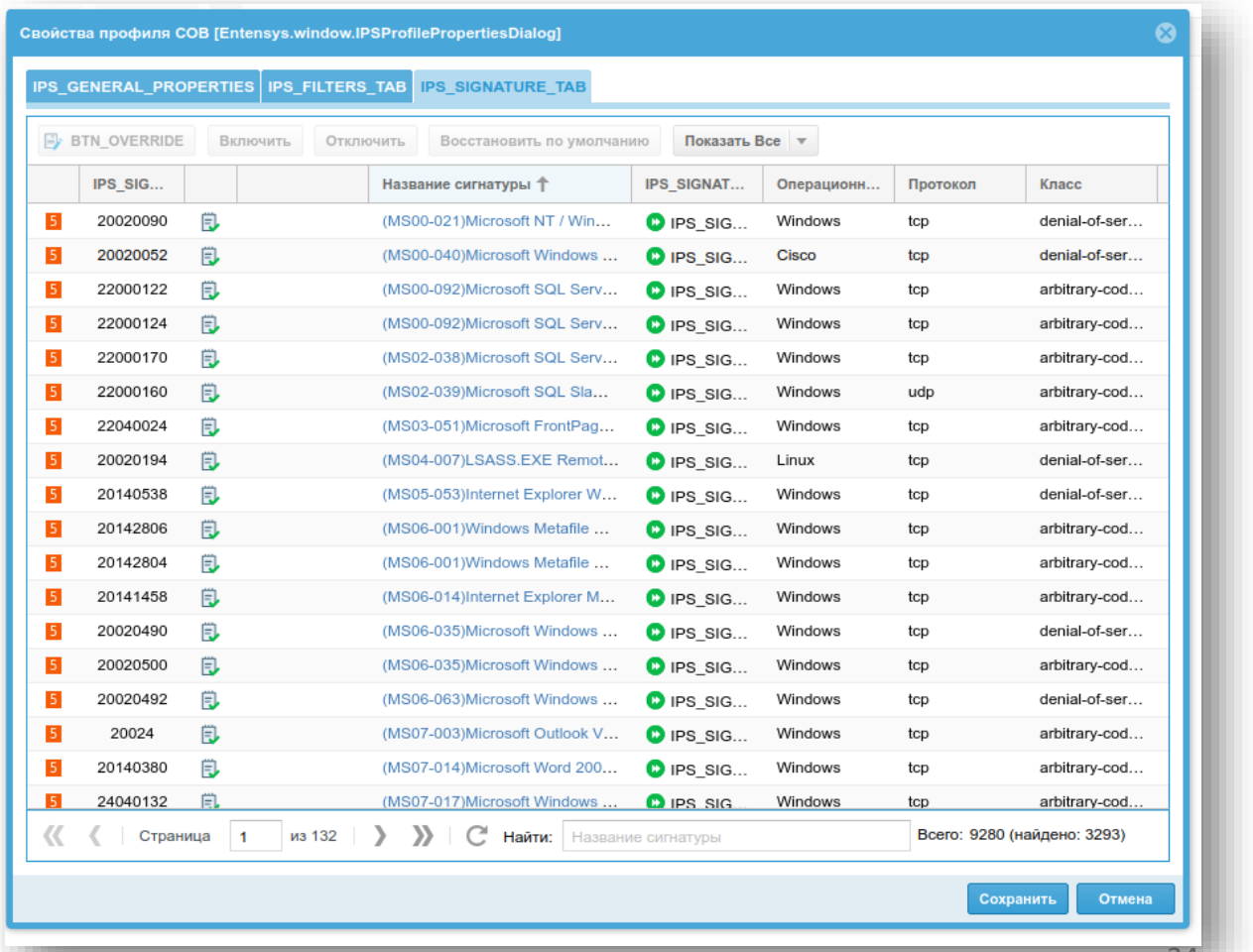

LAN
Any Zone
AD
Login
Actor
WMI
Делаем API-запрос с информацией о пользователе: UID, IP-адрес и список групп для этого пользователя
UserGate Log Analyzer
UserGate NGFW

Создание собственных сигнатур



Создание своего профиля IDPS

с возможностью автоматического обновления
при появлении новых сигнатур соответствующего типа



В рамках UserGate SUMMA

UserGate Client

Endpoint Protection / VPN / EDR / NAC

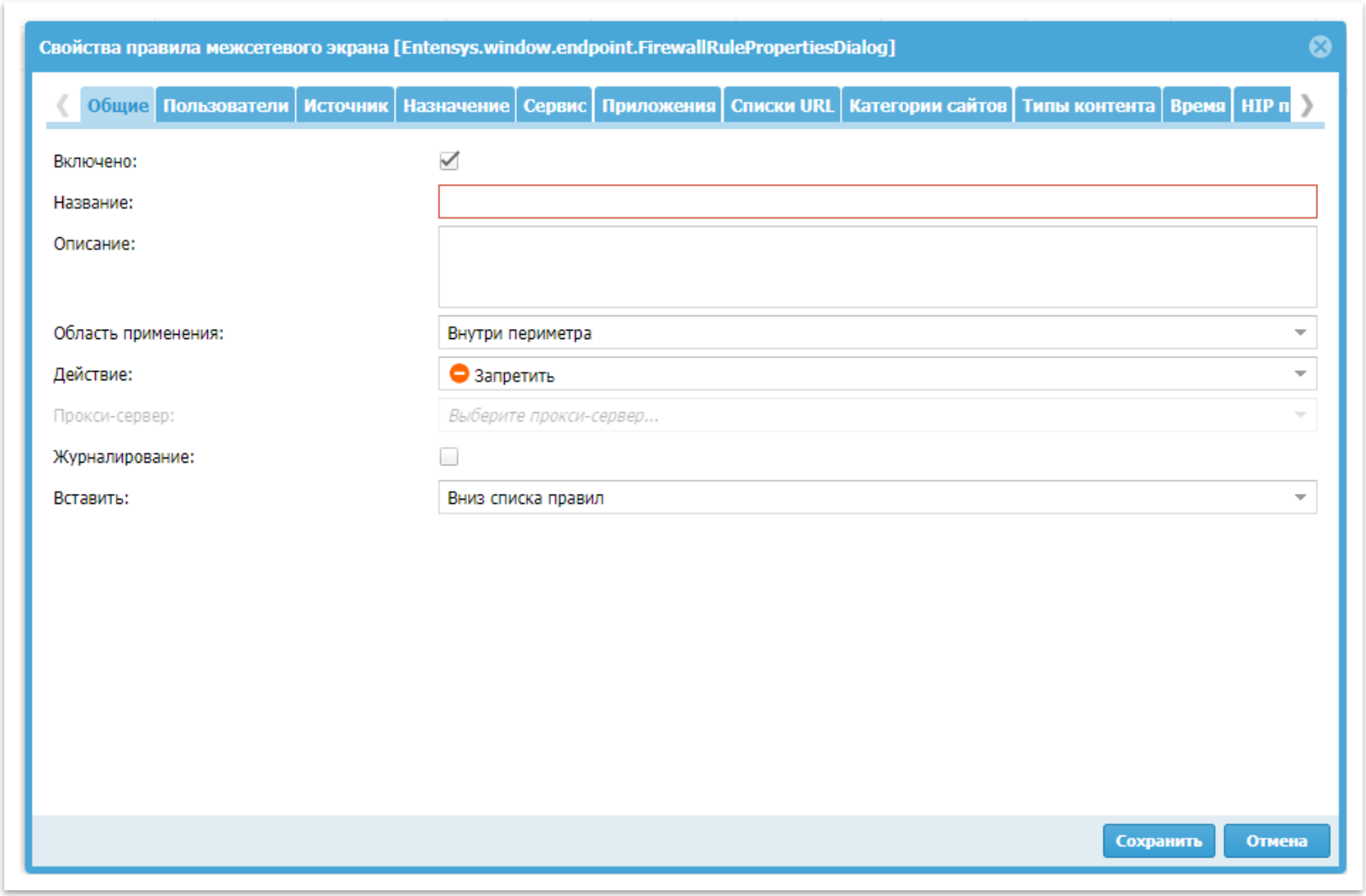
UserGate Client – агент SUMMA

- видимость событий безопасности;
- контроль устройства;
- доступ с нулевым доверием.

Сбор информации с устройства

- состояние, память и производительность;
- безопасность;
- USB-устройства;
- элементы автозагрузки;
- процессы;
- службы;
- ключи реестра;
- программное обеспечение;
- установленные обновления.

Персональный межсетевой экран



NAC

Профили устройств:

- продукт;
- процесс;
- запущенная служба;
- ключи реестра;
- установленные обновления.

VPN

- Client2Site – IPSec/L2TP, IKEv2;
- SSL VPN;
- «принудительный» VPN.

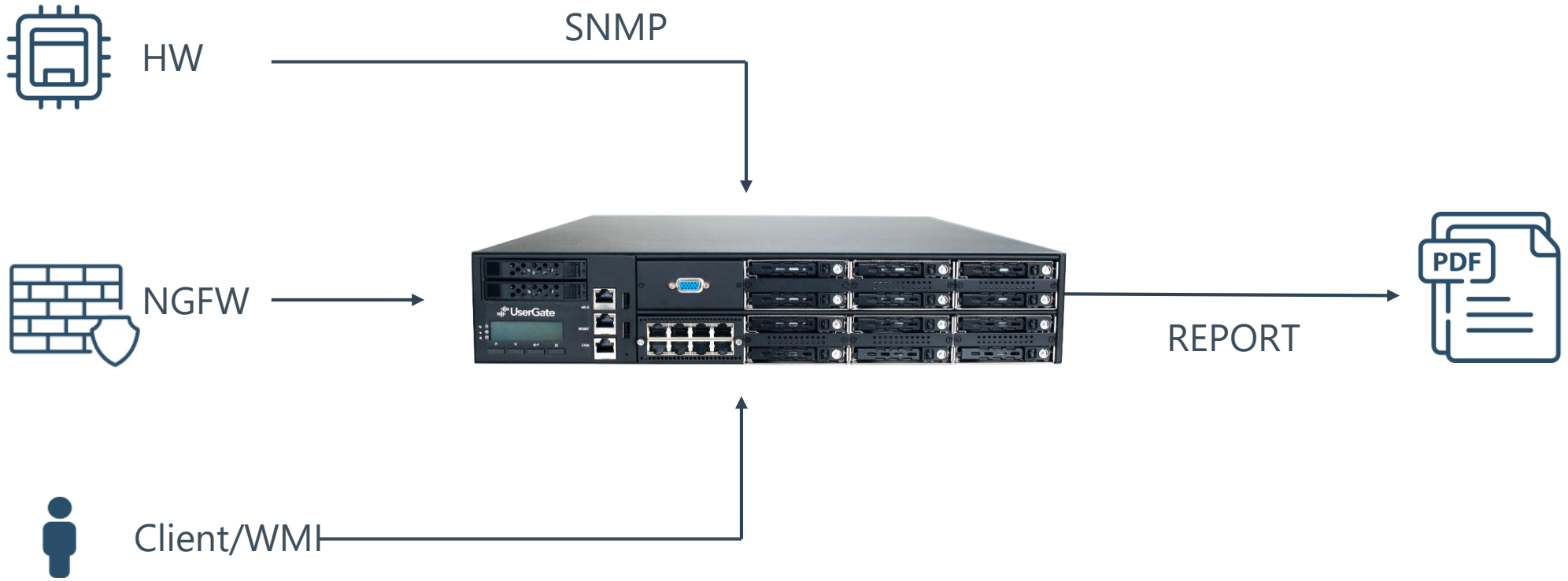
Экспертиза, IoC

Данные из логов, которые можно обогатить и найти следы компрометации:

- IP-адреса;
- домены;
- имена и хеши файлов;
- ветки реестра.

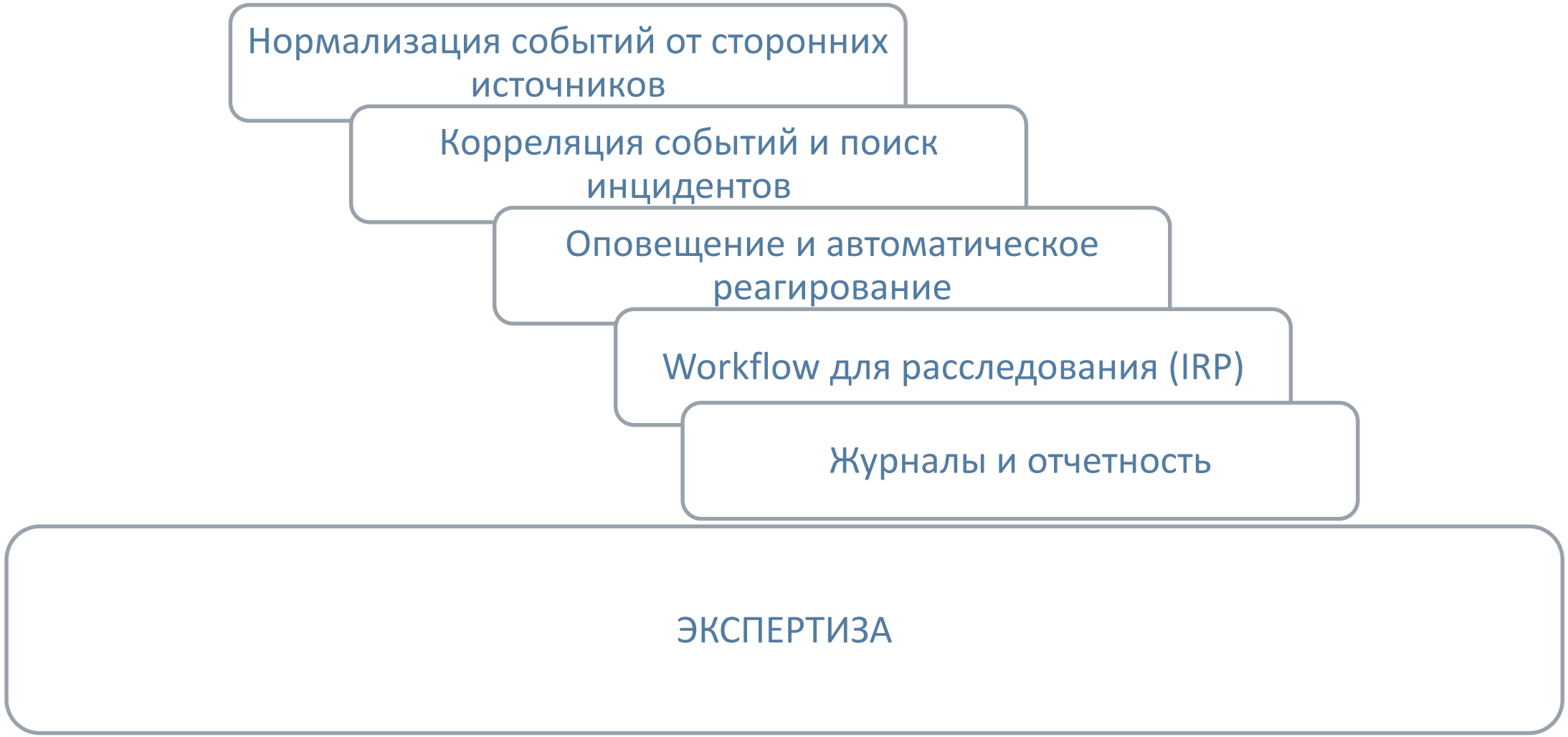
Анализ инцидентов

Анализ инцидентов



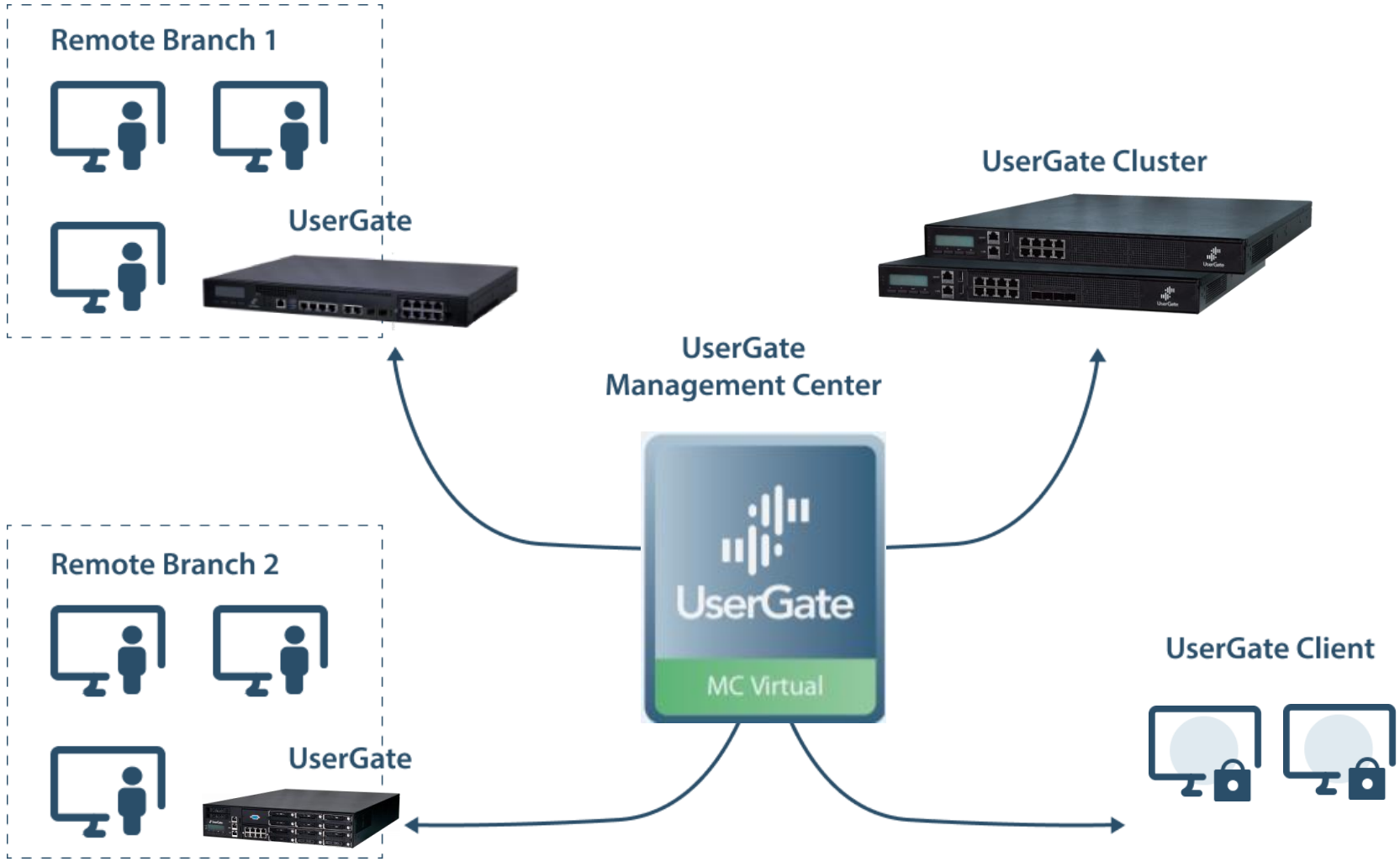
Новый продукт - SIEM Light

Что есть?


Нормализация событий от сторонних источников
Корреляция событий и поиск инцидентов
Оповещение и автоматическое реагирование
Workflow для расследования (IRP)
Журналы и отчетность
ЭКСПЕРТИЗА

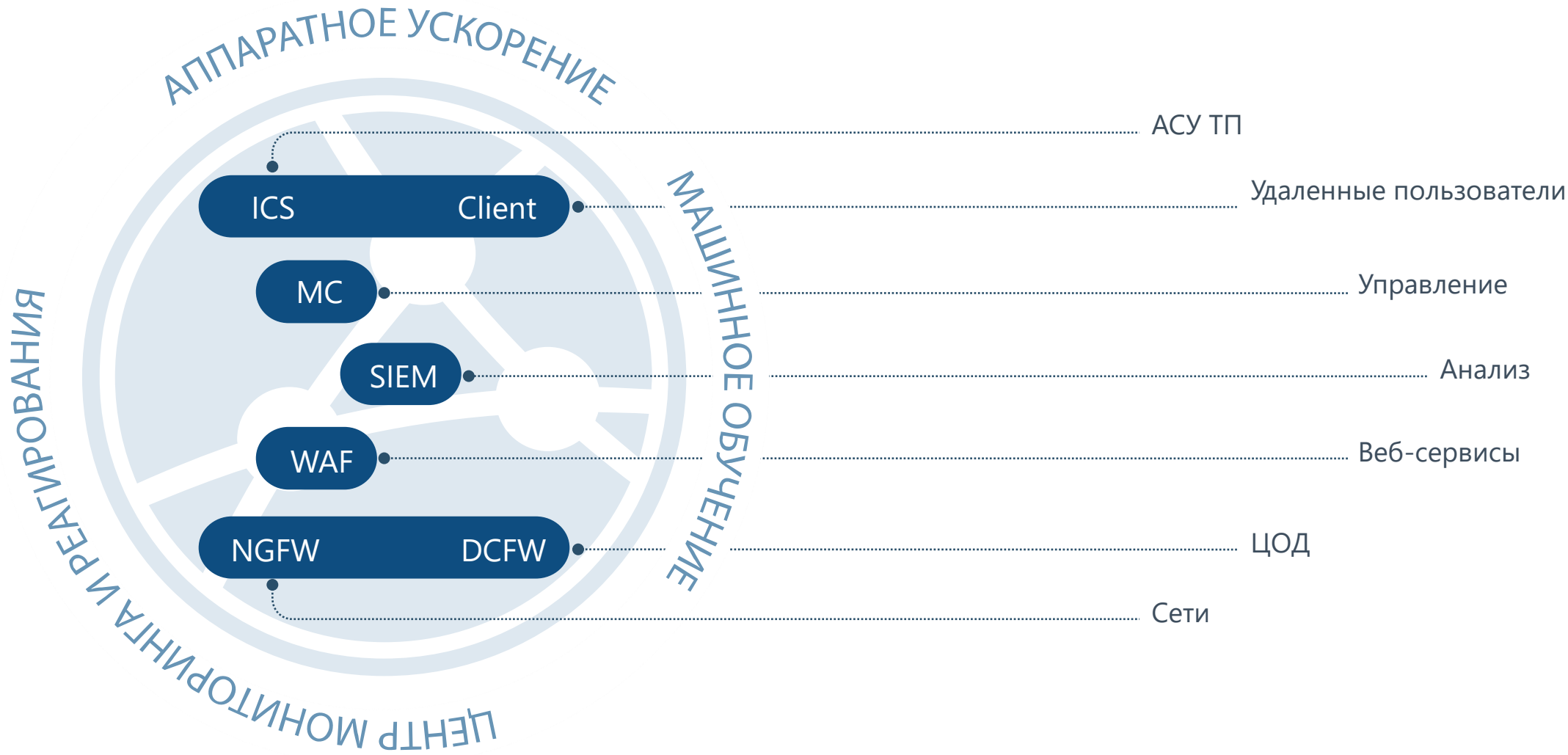
Централизованное управление

Управление устройствами



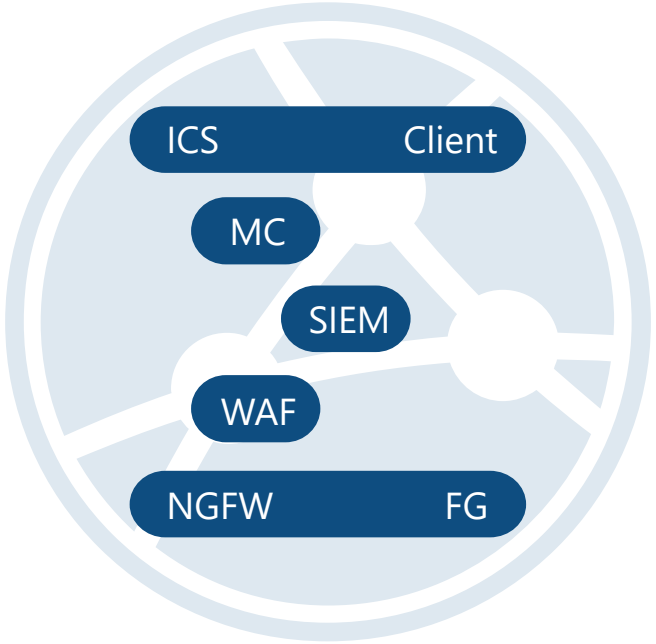
UserGate SUMMA

100% видимость событий безопасности



Формы поставки

Продукты UserGate SUMMA доступны в виртуальном исполнении

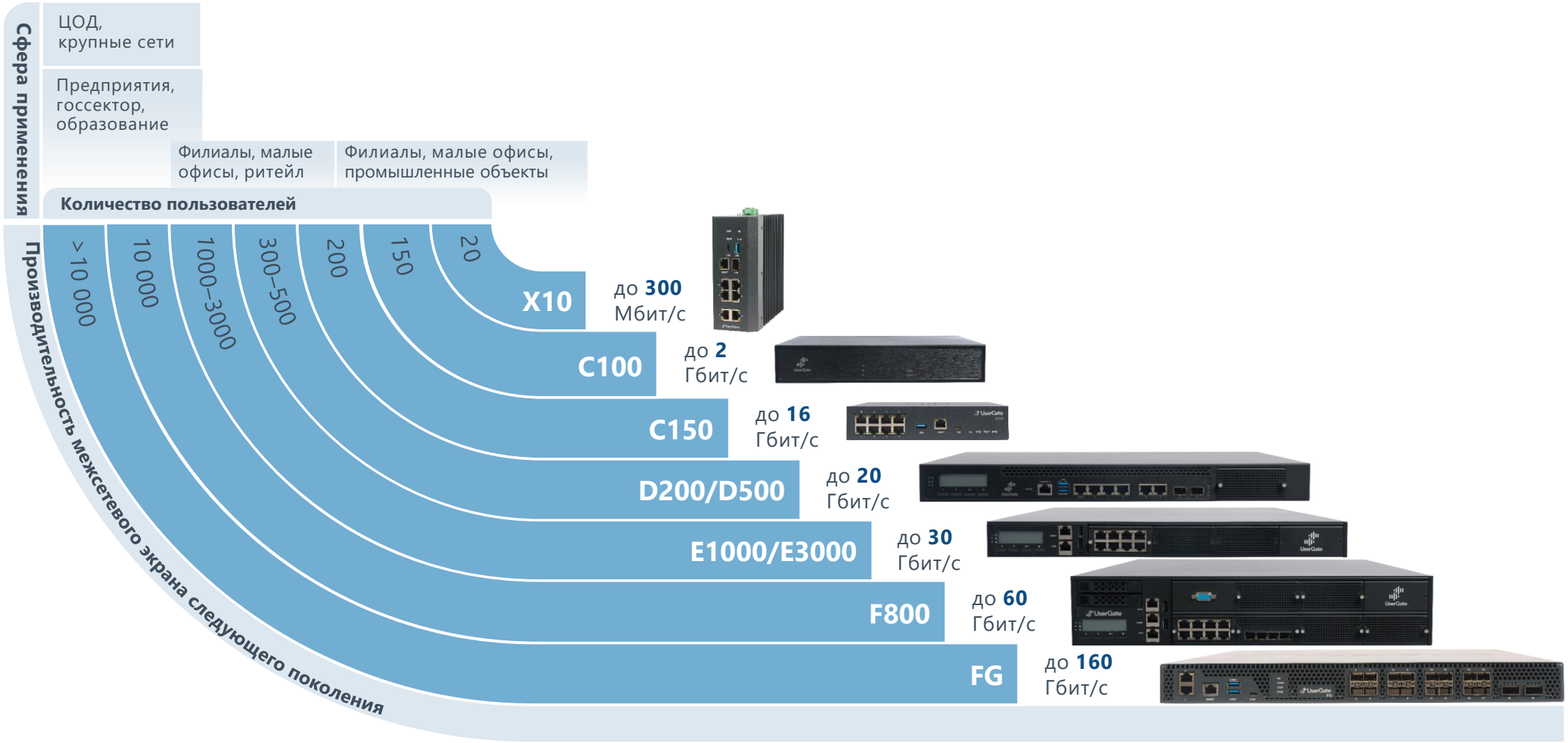


Гипервизоры:

Xen
vmware
Hyper-V
БРЕСТ
ROS ПЛАТФОРМА
base alt
VirtualBox
openstack.
РЕД ВИРТУАЛИЗАЦИЯ
KVM
ГОРИЗОНТ-ВС ЦИФРОВОЕ БУДУЩЕЕ НАЧИНАЕТСЯ СЕГОДНЯ
zVirt

UserGate NGFW

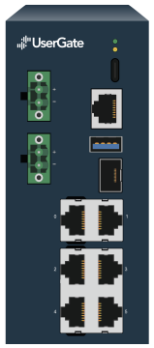
Модельный ряд аппаратных платформ



Собственные разработки железа

Собственные аппаратные платформы

МПТ



Модель X10

- FW до 2,5 Гб/с
- ARM 4 cores
- 6 портов 1GbE с поддержкой bypass
- 1 порт SFP
- два блока питания
- от – 40 °C до +70 °C
- крепление на DIN-рейку

Модель C150

- FW до 8 Гб/с
- ARM 8 cores
- 8 портов 1GbE с поддержкой bypass
- два блока питания
- от 0 °C до +70 °C

Новые платформы

FG

C150

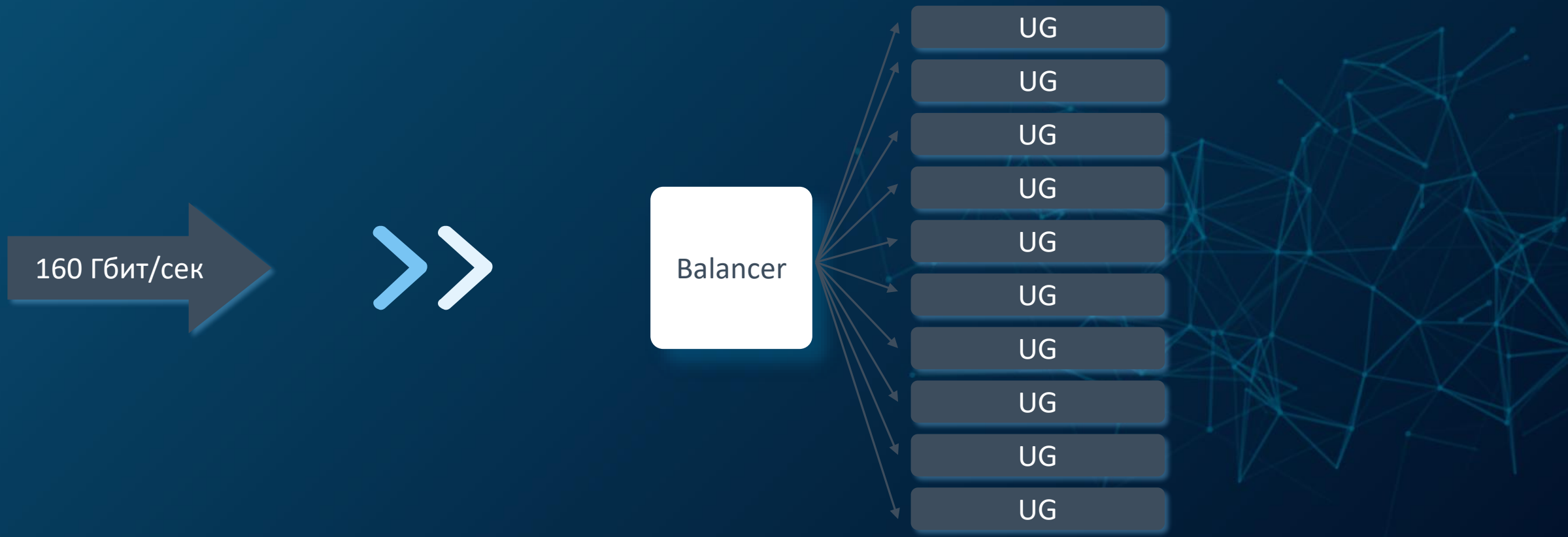
B50

Высокопроизводительный FW

UserGate FG

- CPS - 80 000 сессий в секунду
- CC - 11 000 000 TCP сессий
- UDP 1518 byte - 150+ гбит/с
- EMIX - 65 гбит/с (цифра из ограничения тестового стенда CPS - 35 000, 10 000 правил)
- 80M PPS

2x100 + 16x10, wirespeed


160 Гбит/сек
Balancer
UG
UG
UG
UG
UG
UG
UG
UG
UG
UG

Реализованные проекты

ГБУ РС (Я) Республиканский центр информационных технологий

ПАК UserGate F8000 и UserGate Log Analyzer

- Защита от атак и угроз;
- Безопасный выход в интернет;
- Фильтрация трафика;
- Контроль приложений;
- Анализ событий и инцидентов.

ООО «АльфаСтрахование — ОМС»

Контентная фильтрация web-трафика

- Переход с иностранного вендора;
- Оптимизация оборудования;
- Безопасный выход в интернет;
- Фильтрация трафика.

Пилотирование UserGate

DEMO

Отправьте заявку на пилотирование или запросите демонстрацию решений UserGate

sales@usergate.ru
8 (800) 500-40-32

UserGate

Спасибо
за внимание!