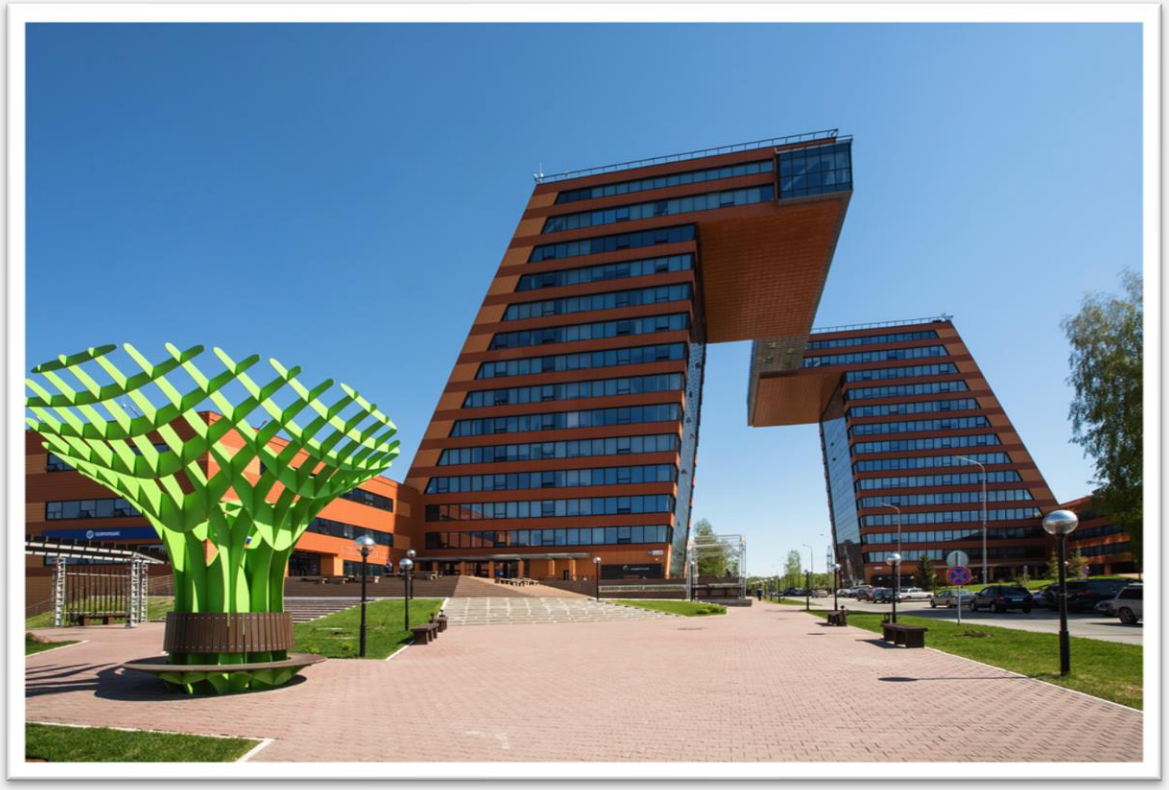
UserGate:
Интернет-безопасность для промышленных предприятий

Антон Рахманенков
ведущий менеджер
по работе с корпоративными клиентами

arakhmanenkov@usergate.com
8 800 500 40 32 | +7-916-720-40-08



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

Дополнительные офисы:
г. Москва, ИЦ «Сколково»
г. Хабаровск

UserGate Log Analyzer

UserGate Management Center

Сетевые функции

Межсетевой экран L7
VLAN, PPPoE, LACP, Bridge
GRE, VXLAN, IP-IP
VRF, Multicast маршрутизация
Routing Static, BGP, OSPF, RIP
NAT, DNAT, PBR
Traffic shaping

Система обнаружения вторжений

L7
СОВ Новый собственный движок
Инспектирование SSL Гранулированная настройка SSL
ГОСТ TLS
ICAP
Инспектирование SSH

Идентификация пользователей

Captive-портал
AD
Kerberos, NTLM, SSO
Radius, TACACS+
MFA

Операционная система UGOS

Безопасность АСУ ТП

L7, IEC 104, Modbus, DNP3, MMS
Новые протоколы
Обработка зеркального трафика

Интернет-фильтрация

Контентная фильтрация
Морфология
Антивирус
Инспектирование SSL

Безопасность почты

Антиспам
Антивирус

Анализ угроз

Поддержка концепции SOAR

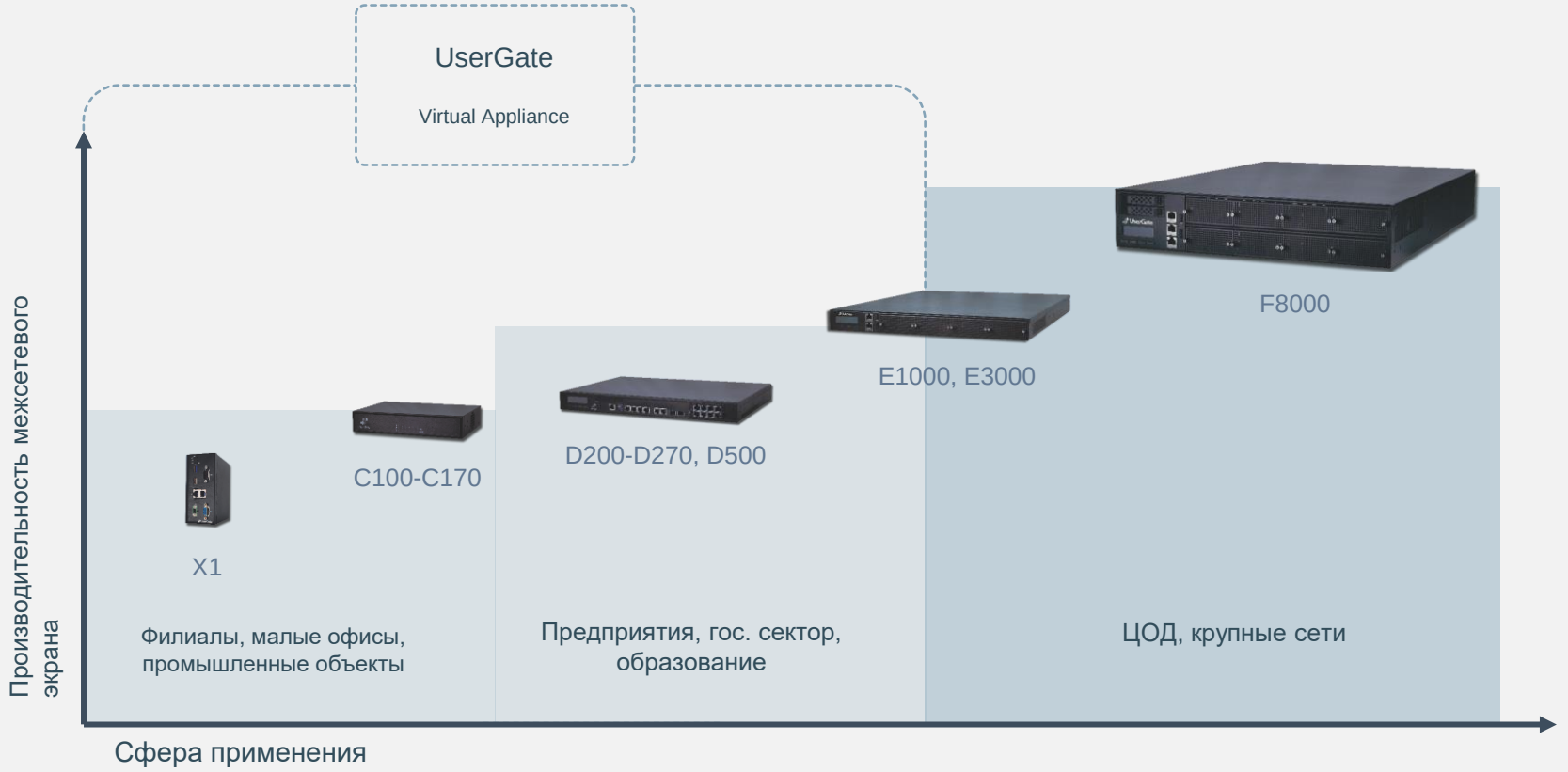
Организация удаленной работы

L2TP IPSec VPN
Совместимость с Cisco VPN
Web-портал (SSL VPN) ГОСТ TLS
Reverse-прокси ГОСТ TLS
Гранулированная настройка SSL

Отказоустойчивость

Кластер конфигурации
Кластер А-А
Кластер А-П

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



Межсетевой экран NGFW

Безопасная публикация ресурсов и сервисов

Система обнаружения и предотвращения вторжений

Анализ команд в протоколах АСУ ТП

Интернет фильтрация

UserGate - Next Generation Firewall

- Сегментирование сети, контроль и анализ трафика между сегментами
- Контроль приложений на L7 уровне по всем портам. Позволяет ограничить трафик для управления сетевыми протоколами и ограниченным набором утвержденных приложений/протоколов для администрирования/сигнализации.
- Идентификация и контроль действий пользователей АСУ ТП (операторов, администраторов, устройств)
- Политика доступа по времени суток вместе с идентификацией приложений и пользователей.
- Возможность централизованного развертывания различных политик и конфигураций на географически распределенных объектах.
- Поддержка ролевой модели доступа.
- Предоставление централизованных отчетов, которые облегчают экспертизу и соблюдение нормативных требований.

Аутентификация 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.

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

Сигнатуры IPS для протоколов АСУ ТП.

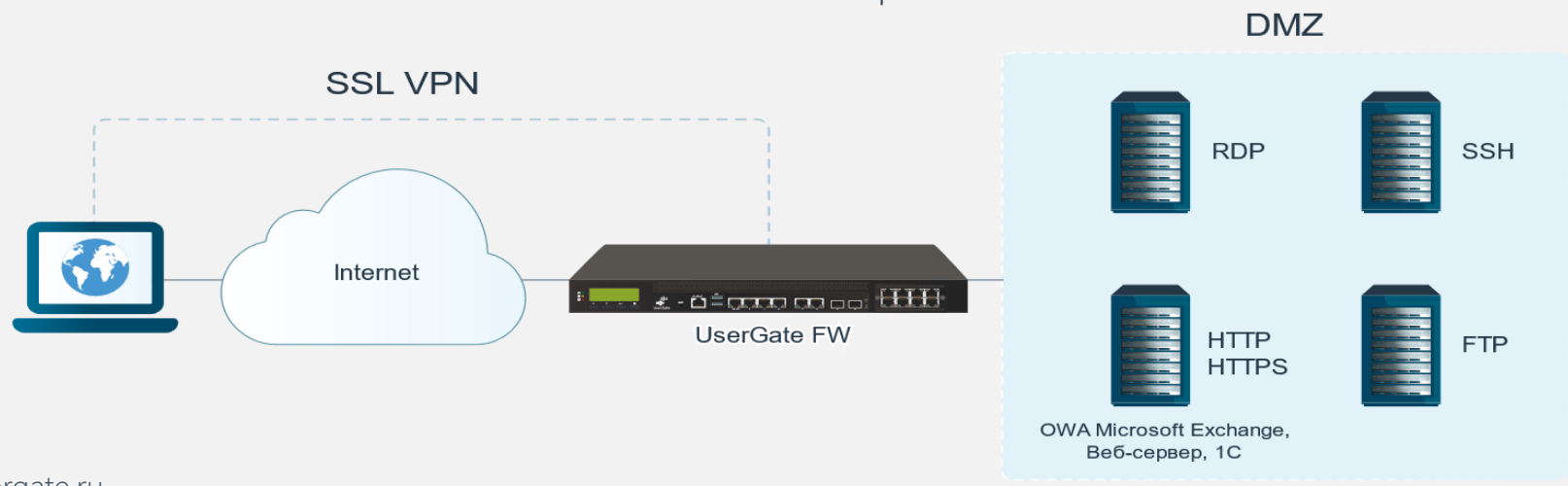
Позволяет реагировать на атаки злоумышленников, использующих известные уязвимости, а также распознавать вредоносную активность внутри сети.

Category: scada ×

Signature	OS	Prot...	Class type	References	Category
Measuresoft ScadaPro Remote Command Executi...	BSD, Linux, Ma...	tcp	arbitrary-code-e...	CVE: 2011-3497	scada
CitectSCADA/CitectFacilities ODBC Server Remot...	Other	tcp	targeted-activity	None	scada
Advantech WebAccess Dashboard Viewer uploadI...	Other	tcp	targeted-activity	None	scada
Advantech WebAccess Multiple Remote Code Exe...	Other	tcp	targeted-activity	None	scada
DATAC RealWin SCADA Server Remote Stack Buf...	Other	tcp	targeted-activity	None	scada
SCADA 3S CoDeSys Gateway Server Directory Tr...	BSD, Linux, Ma...	tcp	arbitrary-code-e...	CVE: 2012-4705	scada
Scadatec Procyon Telnet Service Remote Buffer O...	Other	tcp	targeted-activity	None	scada
Multiple Schneider Electric Products Stack Based ...	Other	tcp	targeted-activity	None	scada
AzeoTech DAQFactory NETB Datagram Parsing B...	None	tcp	targeted-activity	None	scada
CoDeSys Gateway Server CVE-2012-4705 Directo...	Other	tcp	targeted-activity	None	scada
7T Interactive Graphical SCADA System Multiple ...	Other	tcp	targeted-activity	None	scada
ABB MicroSCADA wserver.exe CreateProcessA() ...	BSD, Linux, Ma...	tcp	arbitrary-code-e...	None	scada
ICONICS WebHMI ActiveX Control Stack Buffer O...	None	tcp	targeted-activity	None	scada
Interactive Graphical SCADA System Remote Co...	Other	tcp	targeted-activity	None	scada
Siemens SIMATIC WinCC Default Password Secu...	Other	tcp	default-login-att...	CVE: 2010-2772	scada

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.

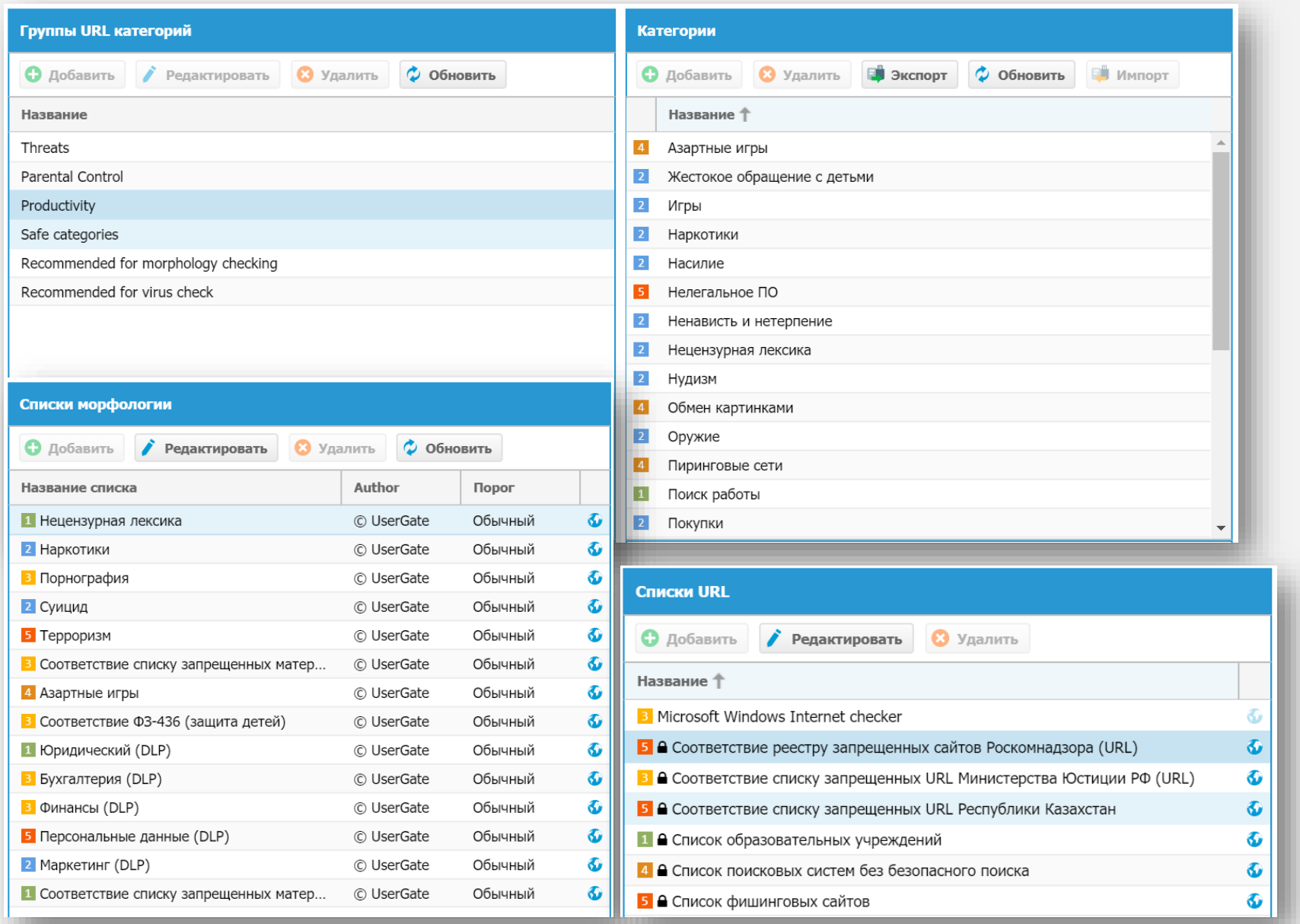
SSL VPN (Веб-портал) – позволяет сотрудникам получить безопасный доступ к корпоративным приложениям через любой браузер, предоставляя удобство использования SSO для опубликованных сервисов, поддерживающих авторизацию по Kerberos, NTLM, SAML в том числе с поддержкой MFA.



Различные механизмы фильтрации:

- фильтрация по категориям (UserGate URL filtering 4.0)
- морфологический анализ
- безопасный поиск
- белые и черные списки
- блокировка контекстной рекламы
- запрет загрузки определенных видов файлов
- антивирусная проверка трафика

- Собственная крупнейшая база электронных ресурсов – более 500 миллионов сайтов
- Более 80 категорий
- Ежедневное обновление списка сайтов
- Повторная проверка уже внесенных ресурсов на предмет изменения контента и актуальности информации о категории

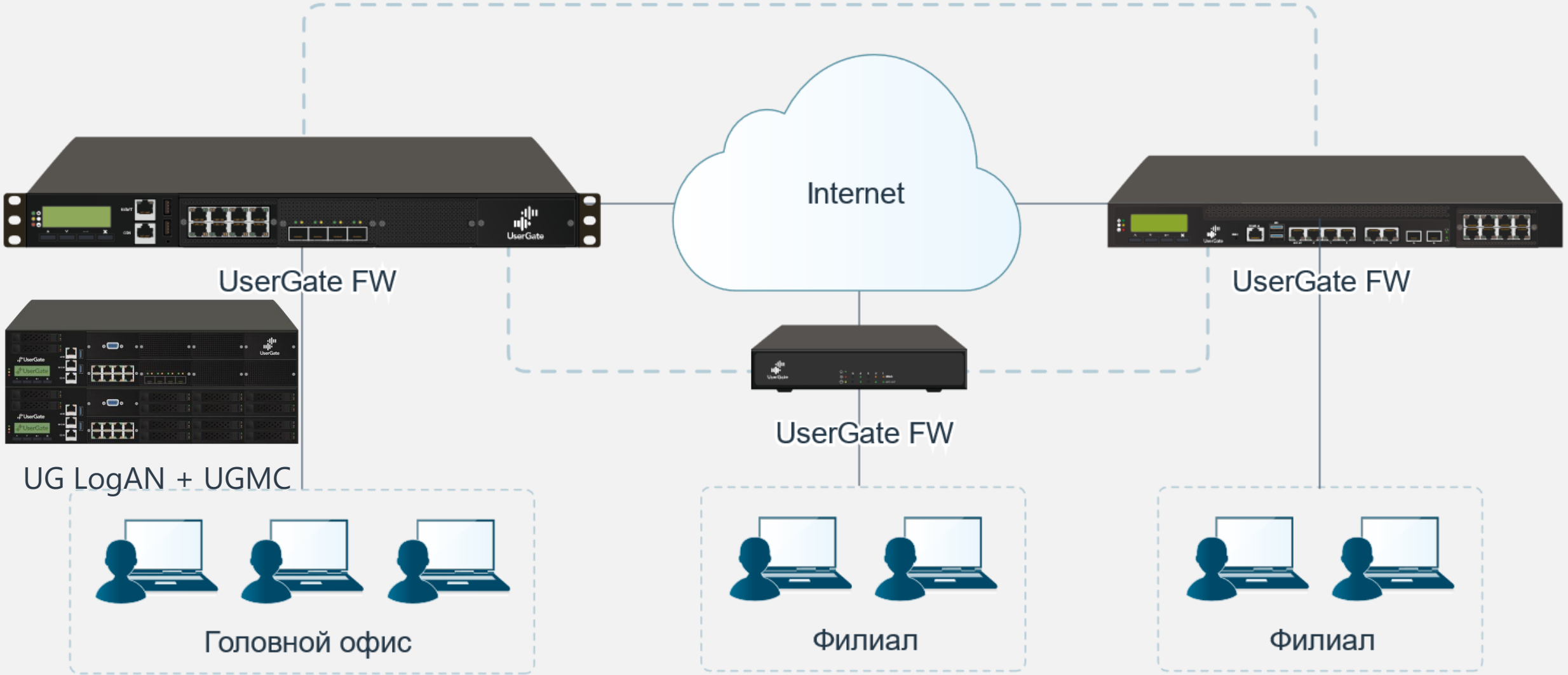


UserGate

UserGate Log Analyzer

Выделенная система сбора, хранения и журналирования логов

- Уменьшение нагрузки на шлюзы UserGate
- Обработка журналов и создание отчетов
- Объединение журналов с нескольких шлюзов для общего анализа
- Увеличение глубины журналирования
- Увеличение размера хранилища на серверах LogAn


Internet
UserGate FW
UserGate FW
UserGate FW
UG LogAN + UGMC
Головной офис
Филиал
Филиал

UserGate

UserGate Management Center

Выделенная система управления NGFW

С помощью UGMC централизованно настраиваются все параметры работы межсетевых экранов UserGate - сетевые настройки, правила межсетевого экранирования, контентной фильтрации, системы обнаружения вторжений и другие настройки. UserGate Management Center позволяет систематизировать подход к составлению настроек через применение шаблонов, а также прозрачно применить эти настройки на выбранной части парка межсетевых экранов.

sales@usergate.ru | usergate.ru

UserGate

Сращивание IT и OT влияют на производство

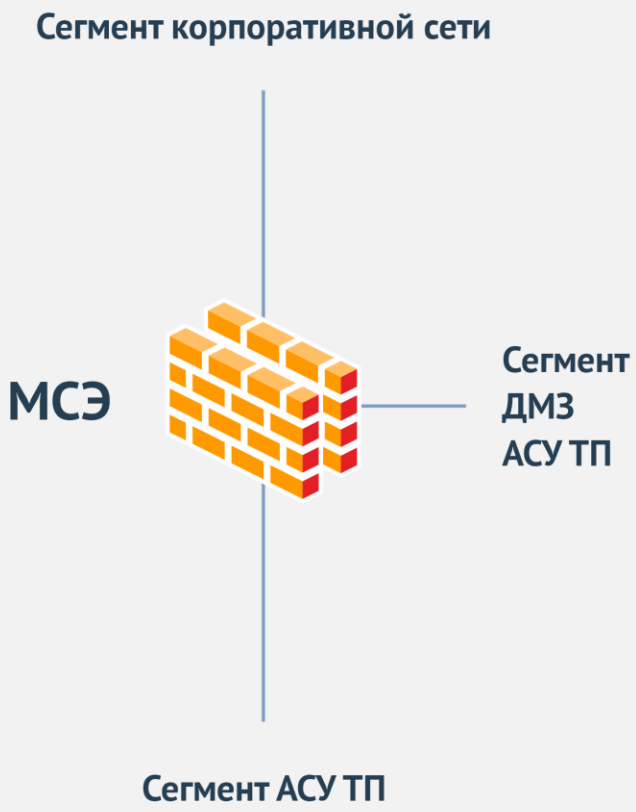
и на множество других областей

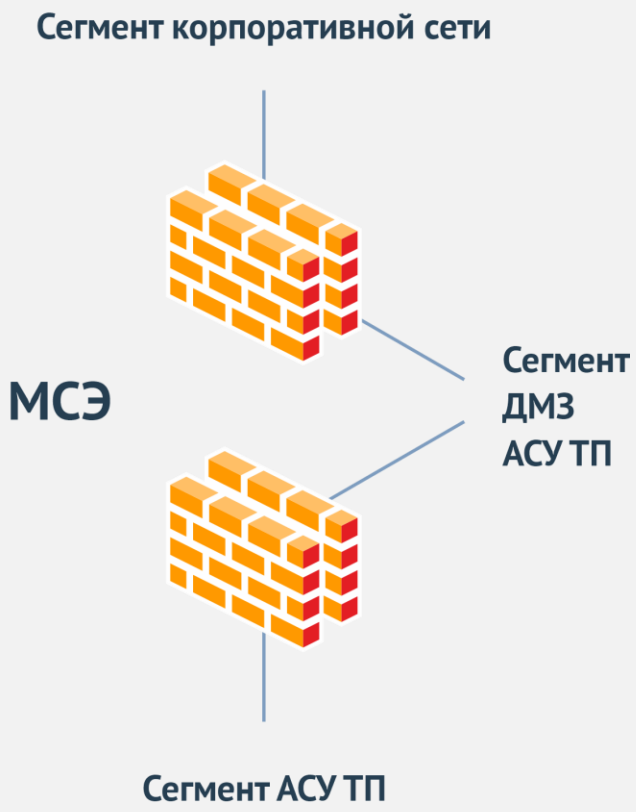
- Управление зданиями
- Энергетика
- Логистика
- Добыча ресурсов
- Нефть и газ
- Умный город
- Водоснабжение
- Химическая промышленность

Угрозы IT	Угрозы OT
Конфиденциальность	Человеческие жертвы Техногенные катастрофы
Целостность	Повреждение оборудования Простои производства
Доступность	Конфиденциальность данных

UserGate

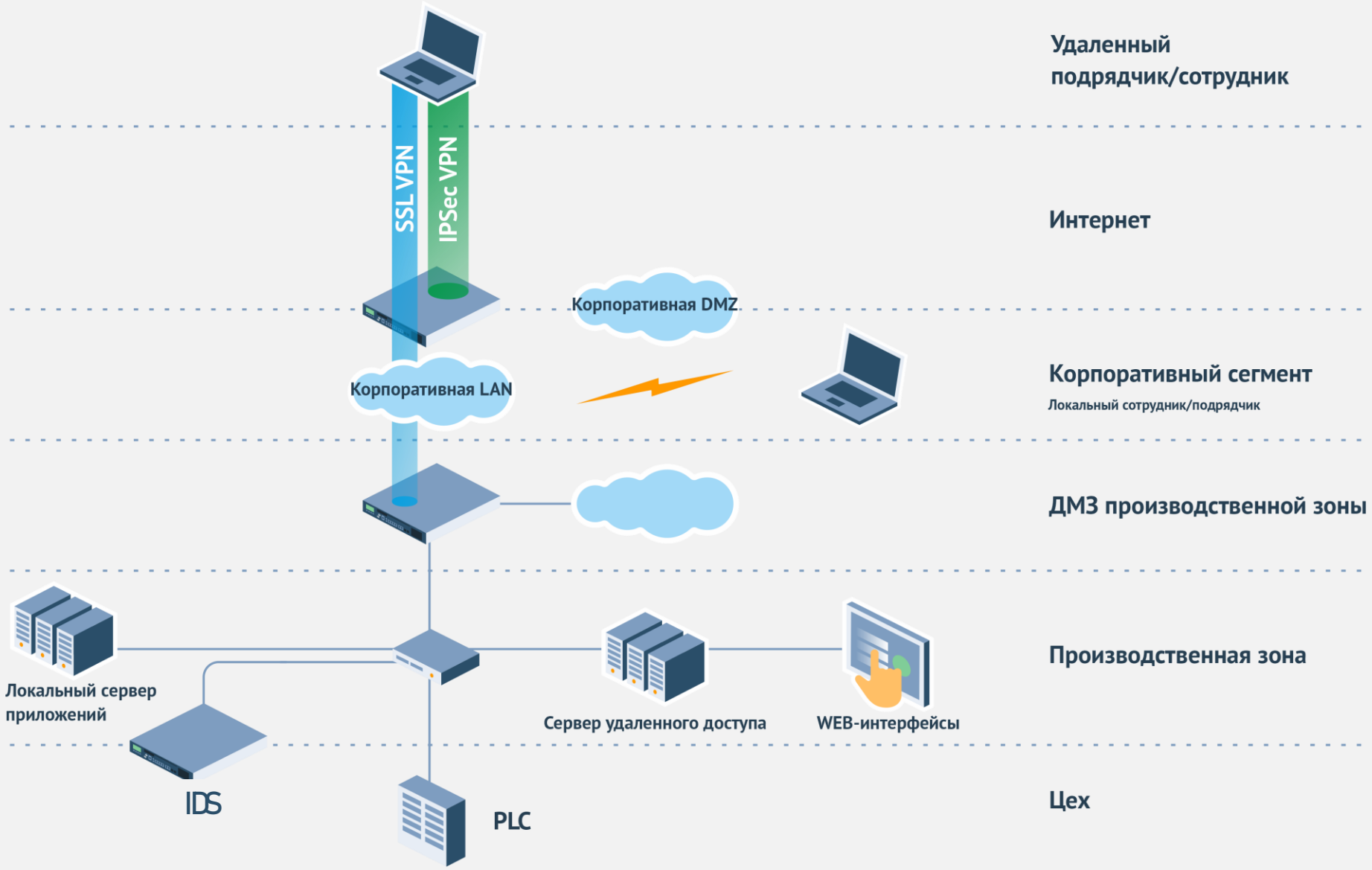
NIST
ISA 99
ГОСТ
МЭК
CpwE





UserGate

Итоговая Архитектура



Стандарт	Контроль на уровне L7	Контроль команд в протоколе
МЭК-61850	✔	✔
IEC 60870-5 ГОСТ Р МЭК 60870-5 IEC 60870-5-104 ГОСТ Р МЭК 60870-5-104	✔	✔
Modbus	✔	✔
DNP3 он же IEEE Std 1815-2010	✔	✔
OPC UA	✔	✔
Ваш протокол	Добавляется по запросу	

Новые платформы UserGate NGFW для АСУ ТП

sales@usergate.ru | usergate.ru

UserGate

Законодательство

Всем производителям СЗИ предписывалось пройти процедуру подтверждения соответствия требованиям к УД до начала 2021 года

Для выполнения требований 17 (ГИС), 21 (ПДн) 31 (АСУ ТП) и 239 (ЗО КИИ) приказов ФСТЭК России необходимо использовать только те СЗИ, которые прошли процедуру соответствия требованиям к УД. Для 239 приказа это требование в полную силу вступает с 2023 года

Кроме того с 2022 года для УД5 и выше сведения об аппаратной платформе должны быть включены в реестр Минпромторга, а с 2028 года для УД4 также сведения о процессорах или микроконтроллерах, элементах памяти, сетевых картах, графических адаптерах

UserGate

Новый сертификат

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;
- АСУТП 1 класса;
- ИСПДн 1 уровня;
- ИСОП II класса

Текст для поиска: Д4 доверия(4)

№ сертификата	Дата внесения в реестр	Срок действия сертификата	Наименование средства (шифр)	Наименования документов, требованиям которых соответствует средство
3905	26.03.2018	26.03.2026	изделие «Универсальный шлюз безопасности «UserGate»	Соответствует требованиям документов: Требования доверия(4), Требования к МЭ, Профиль защиты МЭ(А четвертого класса защиты. ИТ.МЭ.А4.ПЗ), Профиль защиты МЭ(Б четвертого класса защиты. ИТ.МЭ.Б4.ПЗ), Профиль защиты МЭ(Д четвертого класса защиты. ИТ.МЭ.Д4.ПЗ), Требования к СОВ, Профили защиты СОВ(сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ)

1

FORCEPOINT POWERED BY Raytheon
FORTINET
STONESOFT
Barracuda
KerioControl
BlueCoat
McAfee SECURE™
Microsoft Forefront
Check Point SOFTWARE TECHNOLOGIES LTD.

UserGate

АО «НПО «Микроген»

«Микроген» выпускает более 250 наименований лекарственных препаратов на 8 производственных площадках. В качестве замены устаревшему иностранному аналогу в системах безопасности КИИ «Микроген» было выбрано решение UserGate на базе сертифицированных платформ C100 и D500. Задачу глобального мониторинга систем безопасности решает UserGate Log Analyzer. Единой точкой управления информационной безопасностью территориально распределенной IT инфраструктуры предприятия стал UserGate Management Center.

UserGate

ФосАгро

Для доступа в сеть на всех доменных ПК используется технология единого входа (SSO – Single sign-on) и авторизация Kerberos, в основном офисе более 2000 пользователей. Для авторизации при подключении к корпоративному WiFi используется Captive Portal. Для заказчика были разработаны кастомизированные страницы авторизации и блокировки в стилистике компании. Основные задачи, решаемые UserGate UTM состоят в сложной фильтрации http/https трафика по определенным группам пользователей, запрет интернет-ресурсов по категориям, антивирусная проверка трафика на уровне шлюза, фильтрация по спискам. Все эти меры обеспечивают эффективное и безопасное использование интернет-ресурсов работниками компании.

UserGate

ГалоПолимер

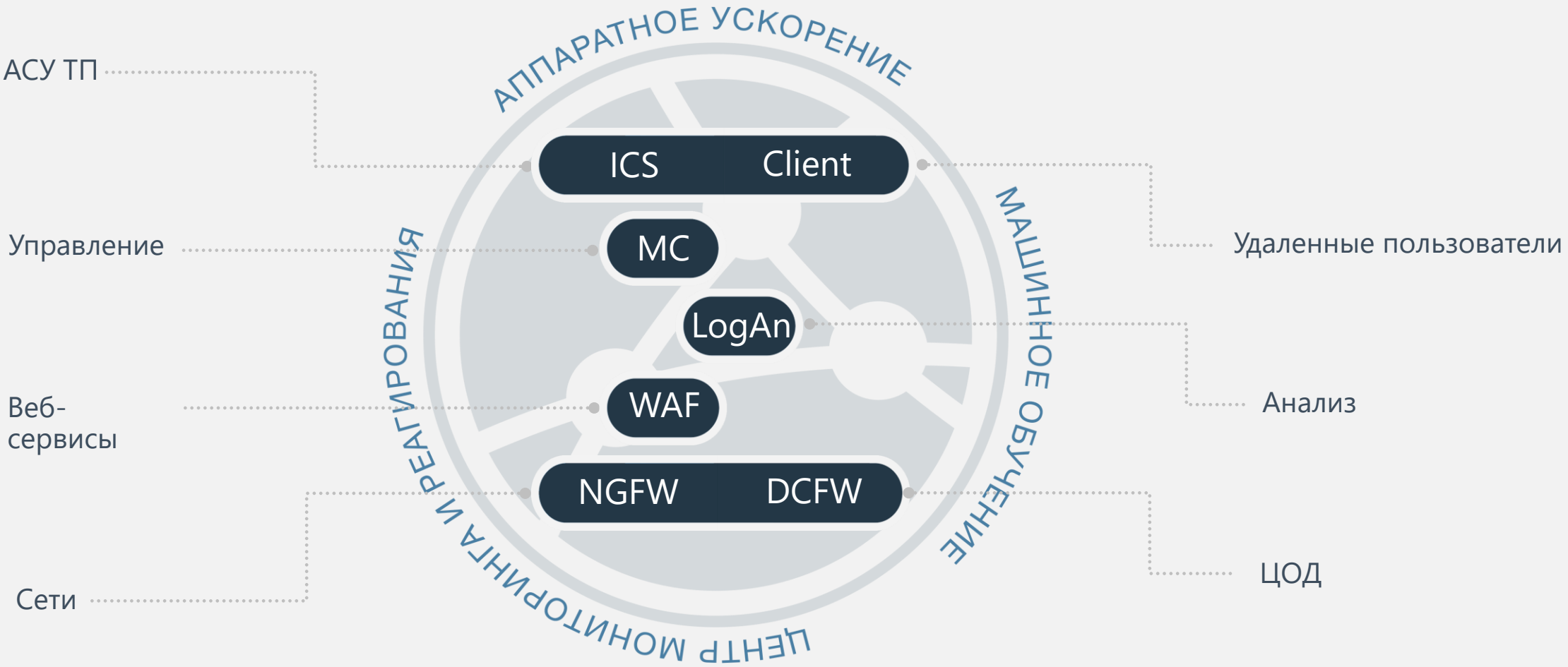
5 площадок, >2000 пользователей.

Анализ трафика сети Интернет по категориям сайтов, URL-адресам и контенту данных. Фильтрация входящего и исходящего Интернет-трафика должна осуществляться с одновременным обеспечением проверки на наличие вредоносного программного обеспечения.

Защита границы периметра сети.

Пилот Management Center.

МИНФИН
РОССИИ


АППАРАТНОЕ УСКОРЕНИЕ
МАШИННОЕ ОБУЧЕНИЕ
ЦЕНТР МОНИТОРИНГА И РЕАГИРОВАНИЯ
ICS
Client
MC
LogAn
WAF
NGFW
DCFW
АСУ ТП
Управление
Веб-сервисы
Сети
Удаленные пользователи
Анализ
ЦОД

UserGate

Благодарим за внимание

Антон Рахманенков

ведущий менеджер
по работе с корпоративными клиентами

arakhmanenkov@usergate.com
8 800 500 40 32 | +7-916-720-40-08