



UserGate SUMMA

Комплексный подход к защите инфраструктуры

Андрей Дуюн

Менеджер по работе с партнерами ПФО

adiun@usergate.ru

+7 913-740-08-18





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 Академпарк в Новосибирске

2019

открытие первого московского офиса UserGate

2018

создание экспертной лаборатории и начало разработки собственных аппаратных платформ

Сертификация новой платформы по требованиям ФСТЭК России

2016

выпуск нового UserGate как решения класса UTM

2015

UserGate – резидент Сколково

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



Решения UserGate для медицины

- Защита от DOS атак
- Защита веб порталов и приложений для внешних пользователей
- Безопасность внутренних сетей от разнообразных внешних интернет-угроз
- Большая зарегулированность
- Безопасность медицинского оборудования (изолировать подсети с трафиком мед оборудования от прочих)
- Проблема с обслуживанием мед оборудования подрядчиками (недоверенное удаленное подключение)



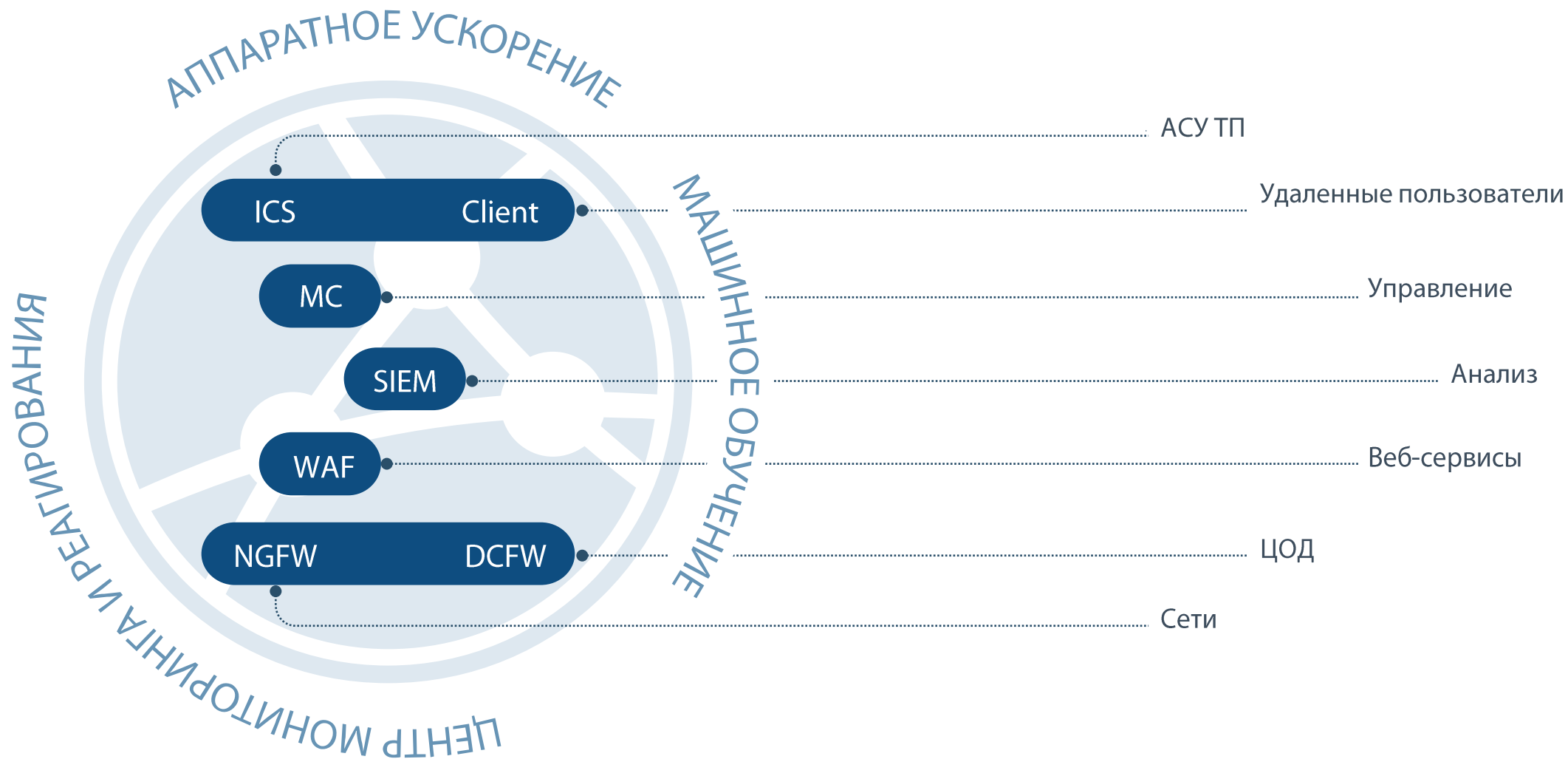
Медицинская организация — субъект КИИ

- идентификация и аутентификация (ИАФ);
- управление доступом (УПД);
- аудит безопасности (АУД);
- антивирусная защита (АВЗ);
- предотвращение вторжений и компьютерных атак (СОВ);
- защита информационной системы и ее компонентов (ЗИС);
- реагирование на компьютерные инциденты (ИНЦ)



UserGate SUMMA

100% видимость событий безопасности





Функционал





UserGate LogAnalyzer
SIEM + IRP, generic rules
ГосСОПКА

UserGate Management Center
Pre- post- rules, UG Client, SIEM

функции UserGate 5, 6, 7 | 7

Сетевые функции

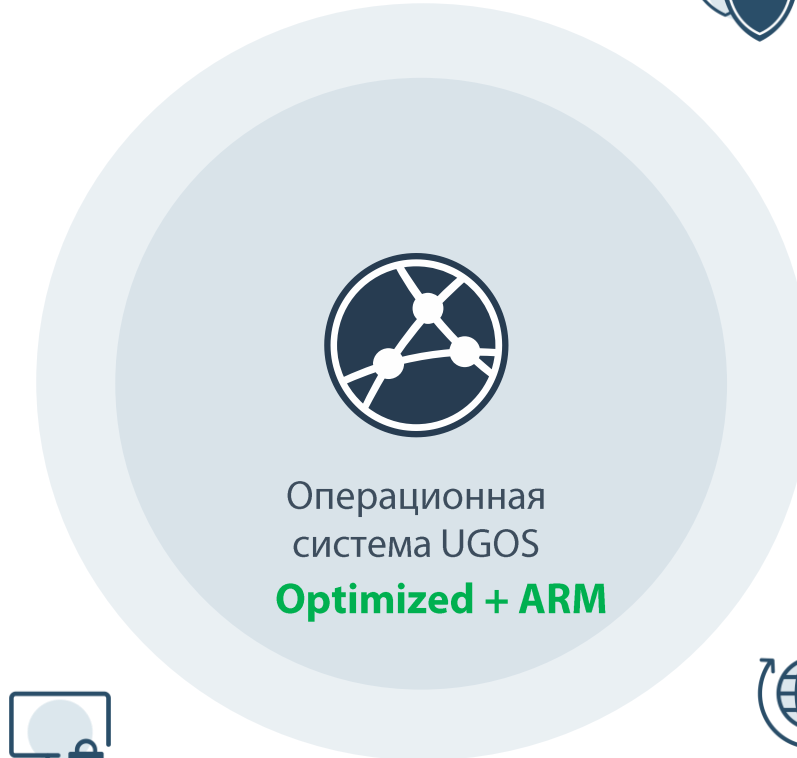
Межсетевой экран **ПРОИЗВОДИТЕЛЬНОСТЬ**
 Разбор трафика на L7
 VLAN, PPPoE, LACP, Bridge
 GRE, VXLAN, IP-IP
VRF, Multicast маршрутизация
 Routing Static, BGP, OSPF, **RIP**
 NAT, DNAT, PBR
 Traffic shaping
 L2 Transparent bridge
LLDP

Идентификация пользователей

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

Интернет-фильтрация

ПРОИЗВОДИТЕЛЬНОСТЬ
 Контентная фильтрация
 Морфологический анализ
 Антивирус (свой)
 Инспектирование SSL



Организация удаленной работы

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



Отказоустойчивость

Кластер конфигурации
 Кластер A-A
 Кластер A-П
 ByPass



Защита от угроз

ПРОИЗВОДИТЕЛЬНОСТЬ
 L7 (hit counters)
 COB **Новый собственный движок, создание собственных сигнатур**
 Инспектирование SSL TLS 1.2 TLS 1.3 **Гранулированная настройка SSL**
Запись трафика при срабатывании
SSL-tap, проверка SSL трафика
ГОСТ TLS
 ICAP
Инспектирование SSH, инспекции GRE, GTP-U и IPSec-незашифрованных туннелей
 Защита от DOS атак
 geo-IP



Безопасность АСУ ТП

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



Безопасность почты

Антиспам



Анализ угроз

Поддержка концепции SOAR

Управление и диагностика

Web Interface
 CLI **все функции, логически отделен от web interface**
 UPL (UserGate Policy Language)
 просмотр и сброс счетчиков интерфейсов, отображение установленных сессий, отображение правил UseGate flow
 Запись трафика в любом направлении
 ARP table
 API XML, REST API
 MC
 поддержка cloud init
 LIVE BACKUP, snapshot



Поддержка АСУ ТП
(SCADA)



Контроль доступа
в интернет



Гостевой портал



Центральная
консоль



Контроль приложений
на уровне L7



Безопасная
публикация ресурсов
и сервисов



Идентификация
пользователей



SIEM UserGate
Log Analyzer



Дешифрование
SSL, SSH



Антивирусная
защита



Контроль мобильных
устройств, поддержка
концепции BYOD



UG Client
EDR, NAC, VPN
Защита конечных станций

UserGate NGFW

Межсетевой экран следующего поколения



Преимущества UserGate NGFW

- 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.

UserGate IDPS (COB)

Модуль в составе UserGate NGFW



Система обнаружения вторжений

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

Поиск

Уровень угрозы	Протокол	Категория	Класс
1 очень низкий	icmp	activex	attempted-user
2 низкий	ip	attack_response	attempted-admin
3 средний	tcp	current_events	attempted-dos
4 высокий	udp	dns	attempted-recon
5 очень высокий		dos	attempted-user
		exploit	bad-unknown
		ftp	default-login-attempt
		imap	denial-of-service
		info	misc-activity
		malware	misc-attack
		misc	network-scan
		mobile_malware	non-standard-protocol
		netbios	not-suspicious
		p2p	policy-violation
		policy	protocol-command-decode

Сигнатуры

Добавить Удалить Обновить

Сигнатура	Прото...	Класс	CVE	Категория
UPDATE Protocol Trojan Communication detected on http ports	tcp	trojan-activity	Her	trojan
dbms_repat.alter_priority_varchar2 buffer overflow attempt	tcp	attempted-user	Her	sql
Suspected CHAOS CnC Inbound (persistence enable)	tcp	trojan-activity	Her	trojan
CygniCon CyViewer ActiveX Control SaveData Insecure Method Vulnerability	tcp	attempted-user	Her	activex
Win32/Infostealer.Snifula File Upload	tcp	trojan-activity	Her	trojan
Possible ZyXEL P660HN-T v1 RCE	tcp	attempted-user	Her	exploit
User-Agent (Win95)	tcp	trojan-activity	Her	malware
STAT overflow attempt	tcp	attempted-admin	CVE-2001-1021,CVE-2001-0...	ftp
Terror EK CVE-2016-0189 Exploit	tcp	trojan-activity	CVE-2016-0189	current_eve
Hazir Site SQL Injection Attempt -- giris_yap.asp sifre UPDATE	tcp	web-application-attack	CVE-2006-7161	web
Rialto SQL Injection Attempt -- searchoption.asp acreage1 INSERT	tcp	web-application-attack	CVE-2006-6927	web

Контент-фильтрация

Модуль в составе UserGate NGFW



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.



Механизмы фильтрации

- Собственная крупнейшая база электронных ресурсов – более 500 миллионов сайтов
- Более 90 категорий
- Ежедневное обновление списка сайтов
- Повторная проверка уже внесенных ресурсов на предмет изменения контента и актуальности информации о категории

Группы URL категорий

Добавить Редактировать Удалить Обновить

Название
Threats
Parental Control
Productivity
Safe categories
Recommended for morphology checking
Recommended for virus check

Категории

Добавить Удалить Экспорт Обновить Импорт

Название ↑
4 Азартные игры
2 Жестокое обращение с детьми
2 Игры
2 Наркотики
2 Насилие
5 Нелегальное ПО
2 Ненависть и нетерпение
2 Нецензурная лексика
2 Нудизм
4 Обмен картинками
2 Оружие
4 Пиринговые сети
1 Поиск работы
2 Покупки

Списки морфологии

Добавить Редактировать Удалить Обновить


Название списка	Author	Порог
1 Нецензурная лексика	© UserGate	Обычный
2 Наркотики	© UserGate	Обычный
3 Порнография	© UserGate	Обычный
2 Суицид	© UserGate	Обычный
5 Терроризм	© UserGate	Обычный
3 Соответствие списку запрещенных матер...	© UserGate	Обычный
4 Азартные игры	© UserGate	Обычный
3 Соответствие ФЗ-436 (защита детей)	© UserGate	Обычный
1 Юридический (DLP)	© UserGate	Обычный
3 Бухгалтерия (DLP)	© UserGate	Обычный
3 Финансы (DLP)	© UserGate	Обычный
5 Персональные данные (DLP)	© UserGate	Обычный
2 Маркетинг (DLP)	© UserGate	Обычный
1 Соответствие списку запрещенных матер...	© UserGate	Обычный

Списки URL

Добавить Редактировать Удалить

Название ↑
3 Microsoft Windows Internet checker
5 Соответствие реестру запрещенных сайтов Роскомнадзора (URL)
3 Соответствие списку запрещенных URL Министерства Юстиции РФ (URL)
5 Соответствие списку запрещенных URL Республики Казахстан
1 Список образовательных учреждений
4 Список поисковых систем без безопасного поиска
5 Список фишинговых сайтов

Безопасная публикация ресурсов и сервисов

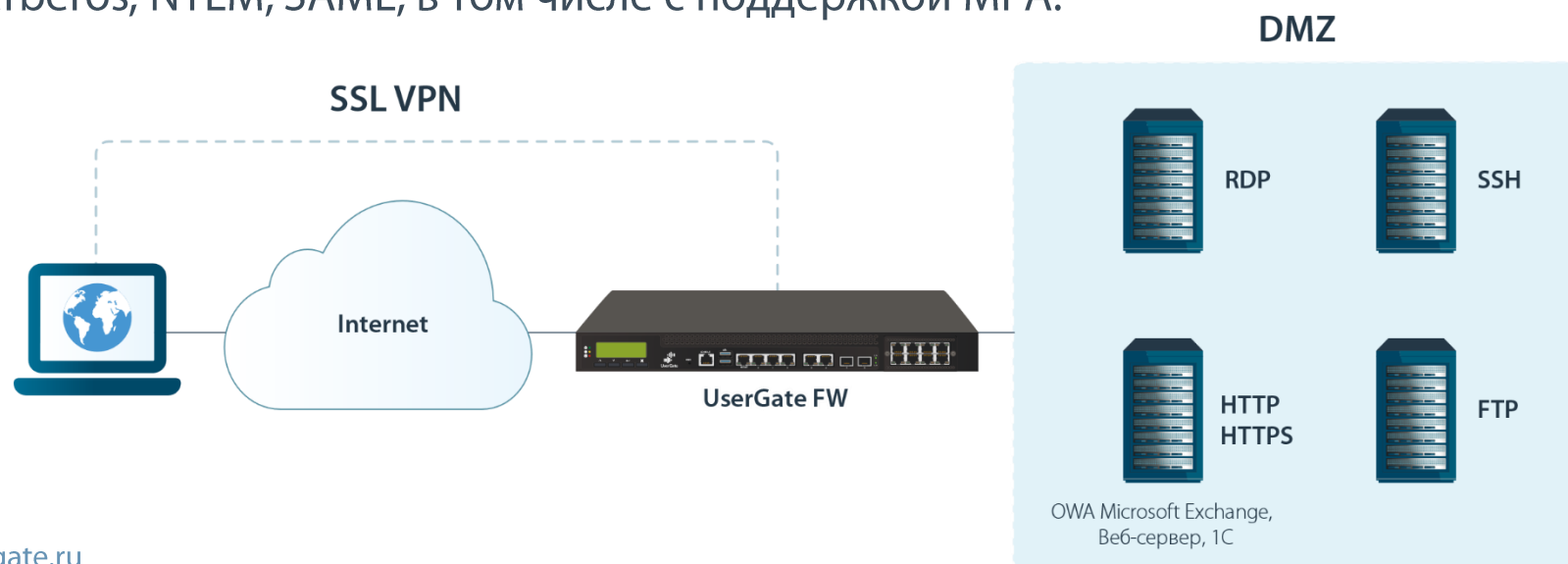
An abstract graphic of a network or web structure, composed of numerous interconnected nodes and lines, rendered in a light blue color against the dark blue background. The network is more densely packed on the right side of the slide and fades out towards the left.



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.





SSL VPN Portal x +

https://sslvpn.mrsk.ru/http/sslvpnportal.local/pp/portal

Поиск

UserGate (user) Выход

Портал SSL VPN 0:00:14

Закладки

Sharepoint portal Outlook Web access RDP server Linux SSH server

Портал Почта web Календарь ВКС Bitrix Terminal access SSH test ИСОТУ

СКИП с паролем Техэксперт СКИП Инструктажи ГИС-Профи

Веб

Адрес: →

История История входов в веб-портал данного пользователя

Login time	IP address	Duration	Operating system
2021/07/09 - 21:30:24	192.168.100.235	12 seconds	Apple Mac
2021/07/09 - 21:29:35	192.168.100.235	16 seconds	Apple Mac



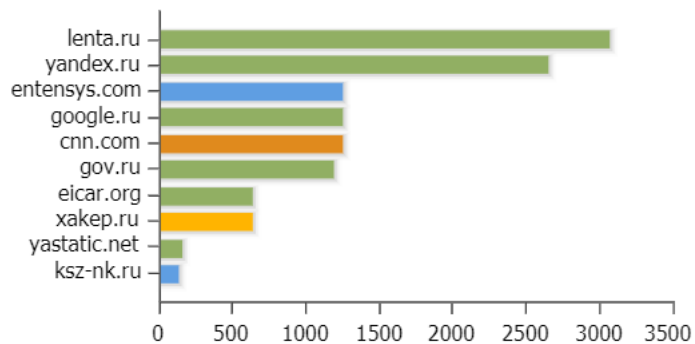
Аналитика и отчетность



Дашборд

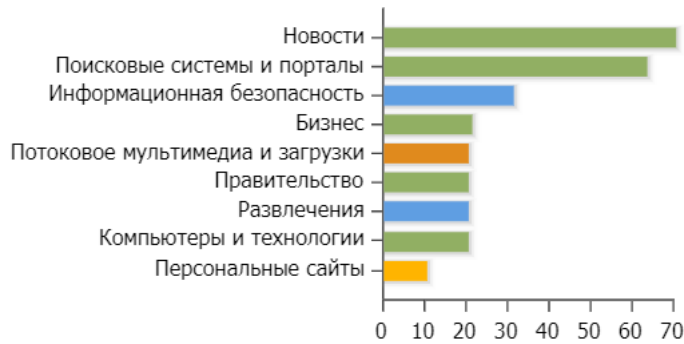
Top 10 domains

Год Месяц Неделя День Сейчас ↻ ⚙ ×



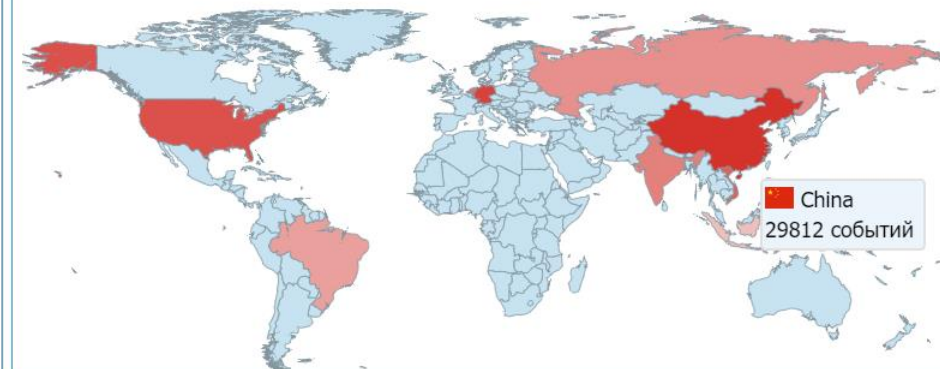
Top 10 categories

Год Месяц Неделя День Сейчас ↻ ⚙ ×



Top 10 attack source countries

Год Месяц Неделя День Сейчас ↻ ⚙ ×



Detected attacks by threat level

Год Месяц Неделя День Сейчас ↻ ⚙ ×

0%

9

2 низкий

79%

6494

4 высокий

21%

1727




5 очень высокий

Last 10 attacks

Год Месяц Неделя День Сейчас ↻ ⚙ ×

Время ↓	×	Сигнатура	IP источника	IP назначения
07:13:58	📅	4 Suspicious inbound to M...	🇨🇳 103.94.123.206	🇩🇪 138.68.85.159
07:13:55	📅	4 Suspicious inbound to M...	🇨🇳 221.194.44.208	🇩🇪 138.68.85.159
07:13:51	📅	4 Suspicious inbound to M...	🇨🇳 125.161.72.33	🇩🇪 138.68.85.159
07:12:52	📅	5 ntpdx overflow attempt	🇫🇷 51.159.59.122	🇩🇪 138.68.85.159
07:08:02	📅	5 Suspicious User Agent (...)	🇩🇪 138.68.85.159	🇷🇺 178.248.232.27
07:08:02	📅	5 Suspicious User Agent (...)	🇩🇪 138.68.85.159	🇷🇺 81.19.72.59
06:52:35	📅	5 Potential MySQL bot sca...	🇷🇺 87.251.74.9	🇩🇪 138.68.85.159

Правила отчетов

Правила отчётов									
+ Добавить ✎ Редактировать ✖ Удалить 📄 Копировать 🔘 Включить 🔘 Отключить ▶ Запустить сейчас 🔄 Обновить Показать Все ▾									
✕	Название ↑	Пользователи	Диапазон	Количество...	Количество в гру...	Шаблоны отчёта	Расписание	Профили SMTP	Emails
	Captive portal report	Любой	Текущий ме...	100	5	Авторизация через... Авторизация через... Авторизация через... Авторизация через... ...	5 0 * * *	Нет	Нет
	IDPS report	Любой	Текущий год	100	5	Топ сигнатур COV ... Сработавшие сигн... Срабатывания COV... Срабатывания COV... ...	5 0 * * *	Нет	Нет
	Network policy report	Любой	Текущий год	10	5	Топ сработавших п... Блокирующие прав... Пользователи по б... Блокирующие прав... ...	5 0 * * *	Нет	Нет



Management Center





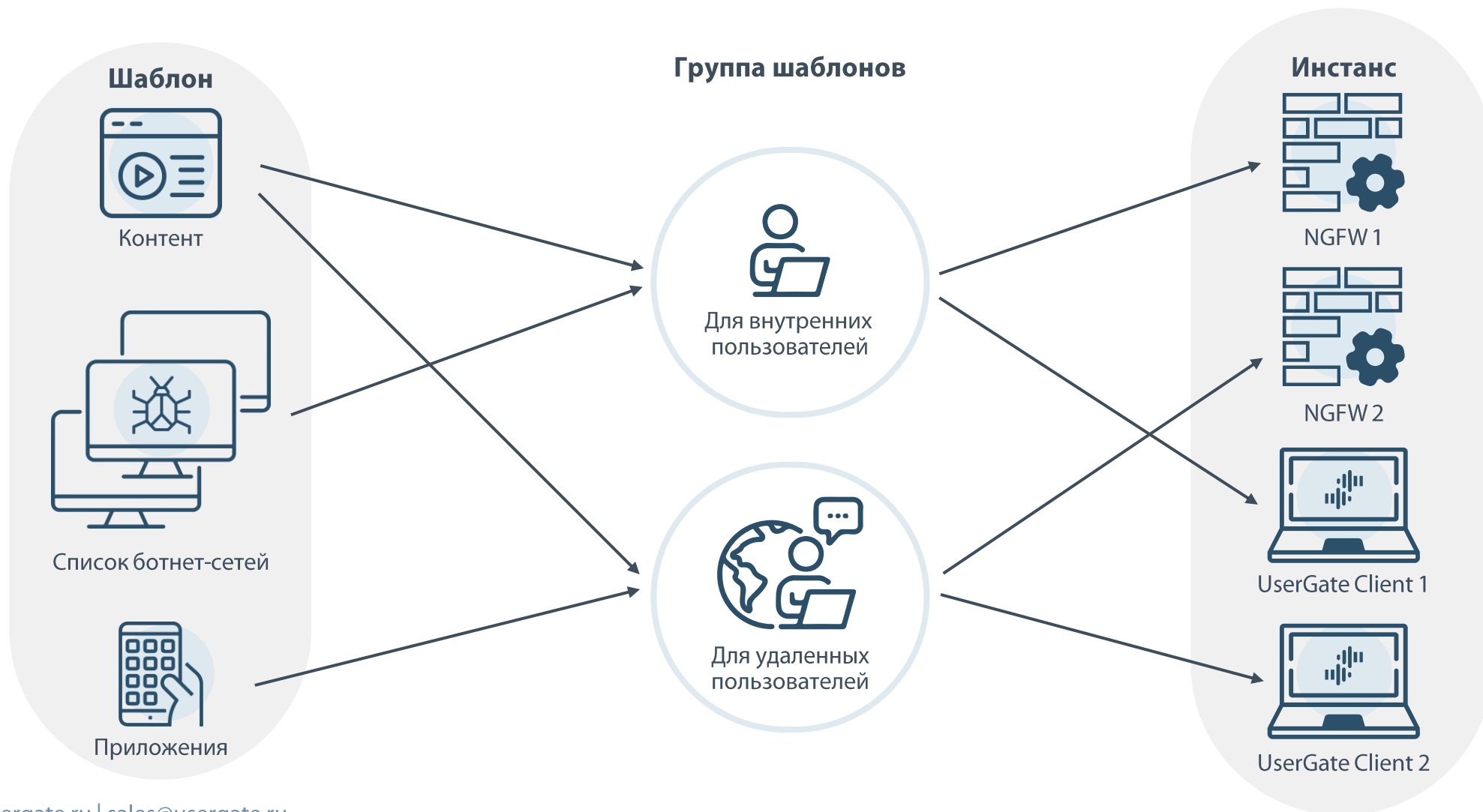
UserGate Management Center – зачем?

- упрощение администрирования большим парком продуктов UserGate (управление списками объектов: IP-адреса, URL-адреса, морфология, типы контента и т.д.);
- централизованное управление политиками безопасности и шаблонами политик безопасности;
- ролевая модель доступа к управлению;
- создание мультитенантной среды.



Шаблоны

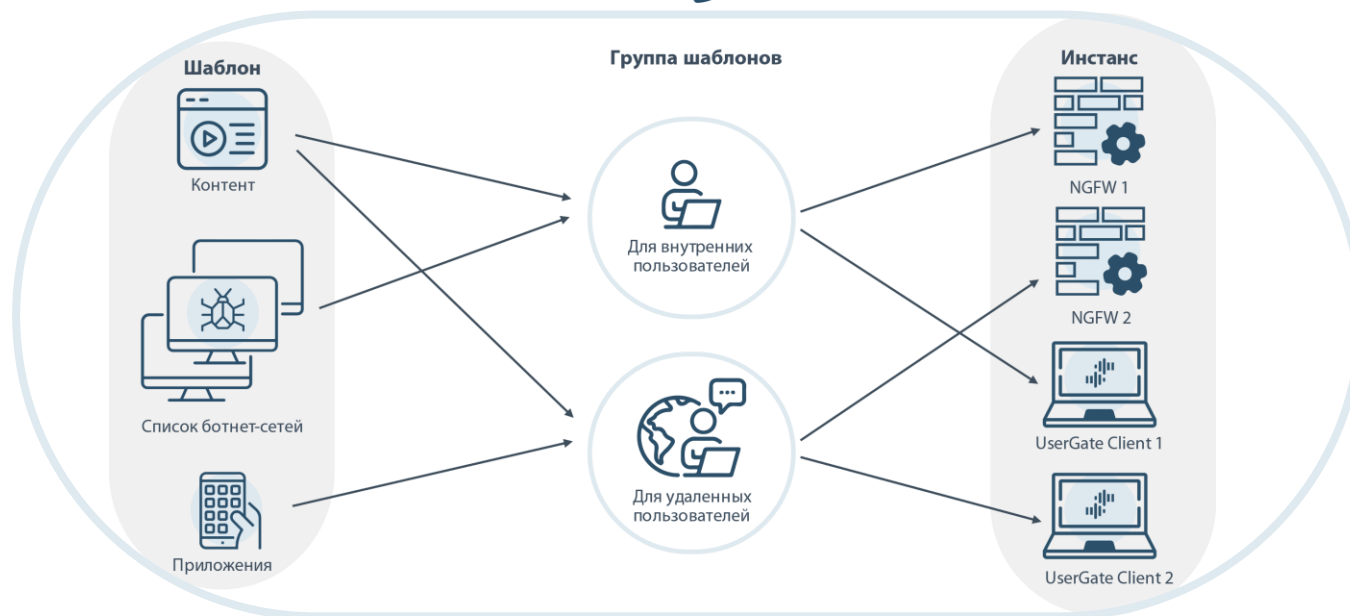
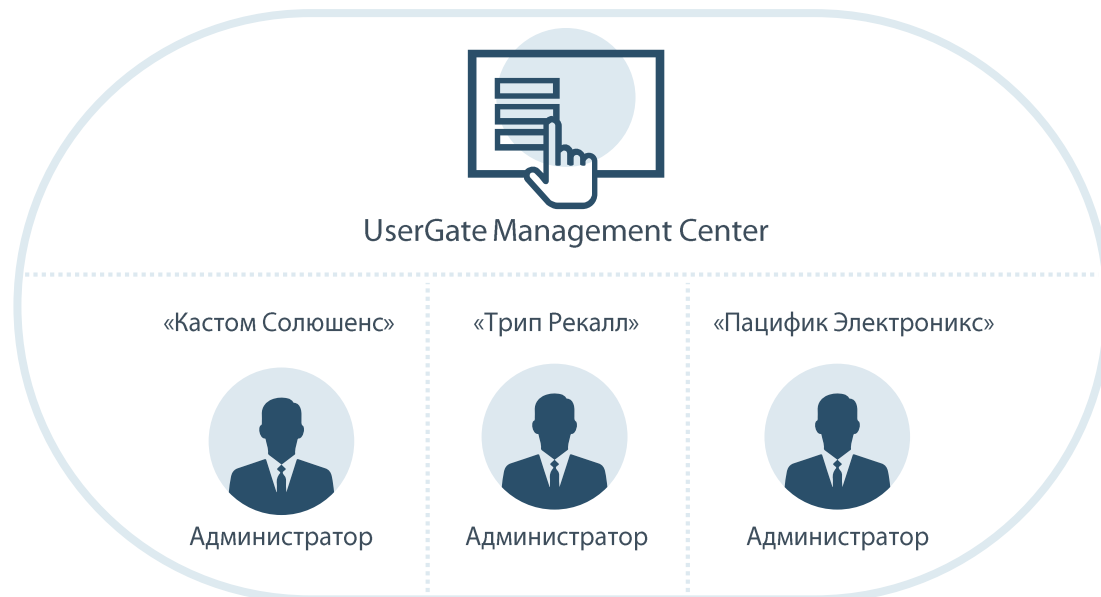
Management Center позволяет создавать шаблоны политик безопасности.





Области

- для управления ДЗО;
- для обслуживающих организаций;
- для облачных/MSSP-поставщиков.



Здравый смысл





Выбор очевиден



Более 2000 реализованных проектов в разных сферах



Транспорт



Связь



Сфера атомной
энергии



Металлургическая
промышленность



Химическая
промышленность



Здравоохранение



Банки
и финансовые
организации



Горнодобывающая
промышленность



Наука



Энергетика
и топливно-энергетический
комплекс



Ракетно-
космическая
промышленность



Оборонная
промышленность



Органы власти



Образовательные
учреждения



Торговые сети



Малый и средний
бизнес





Пилотирование UserGate



DEMO

Отправьте заявку на пилотирование или
запросите демонстрацию решений UserGate

adiun@usergate.com

8 (913) 740-08-18



**Спасибо
за внимание!**

Андрей Дуюн

Менеджер по работе с партнерами ПФО

adiun@usergate.ru

+7 (913) 740-08-18

