UserGate SUMMA – слагаемые комплексной безопасности

Александр Богданов
Партнерский отдел UserGate

abogdanov@usergate.com
+7 (800) 500 40 32 доб. 1033 | +7 (913) 792 61 48

До 2010 года

Компания Entensys разрабатывала популярные программные решения под Windows-платформу для малого и среднего бизнеса

2010 год

Создан внутренний стартап, в рамках которого началась разработка новой платформы

2013 год

Выпущено решение UserGate Web Filter для операторов связи и публичного WiFi, университетов и школ

2016 год

Выпущен UserGate UTM, комплексное решение для обеспечения безопасности корпоративных сетей

2018 год

Создана новая лаборатория и начата разработка собственных аппаратных платформ. Пройдена сертификация ФСТЭК.

2020 год

UserGate стал решением уровня Next Generation Firewall. Реализовано несколько тысяч проектов, в большинстве из которых замещены зарубежные аналоги.

2021 год

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. Хабаровск
* г. Санкт-Петербург

Основа для развития –
это лучшие технологии

Во время повсеместного использования открытого кода мы всегда полагаемся только на **собственные разработки** и полностью **контролируем свое решение**

В компании **UserGate** мы разрабатываем не только ПО, **мы разрабатываем всю платформу целиком**

UserGate

БЕЗОПАСНОСТЬ – ЭТО СЛОЖНО

Remote Access

Периметр и сегментация

IDPS

Безопасность АСУ ТП

Анализ и управление

Интернет фильтрация

Защита почты

Антивирус

Remote Access

ZTNA

Периметр и сегментация

IDPS

SASE

Безопасность АСУ ТП

Анализ и управление

XDR

SOAR

Интернет фильтрация

NGFW

Защита почты

Антивирус

NAC

UserGate

L4 =/= ШЛЮЗ БЕЗОПАСНОСТИ

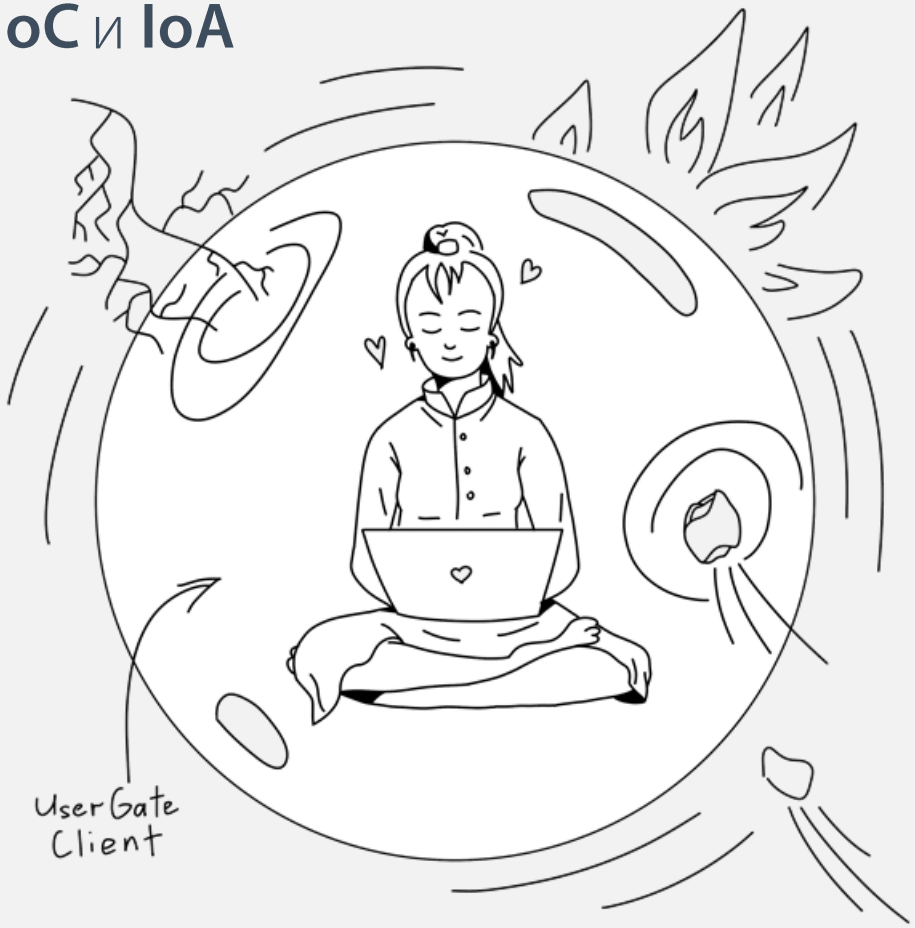
- Правила по пользователям и приложениям
- Не только детект, но и превент
- Максимальная видимость

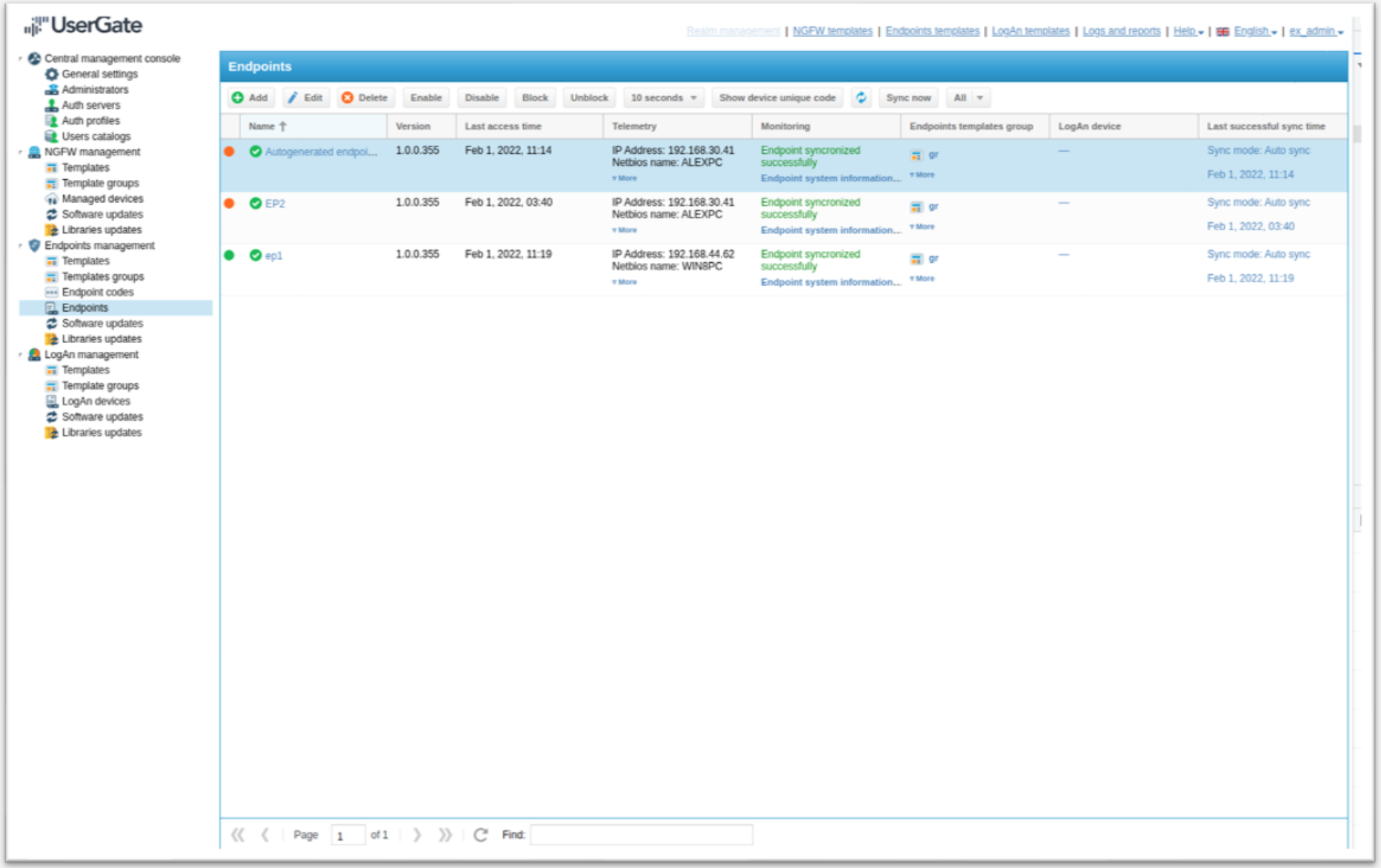
UserGate

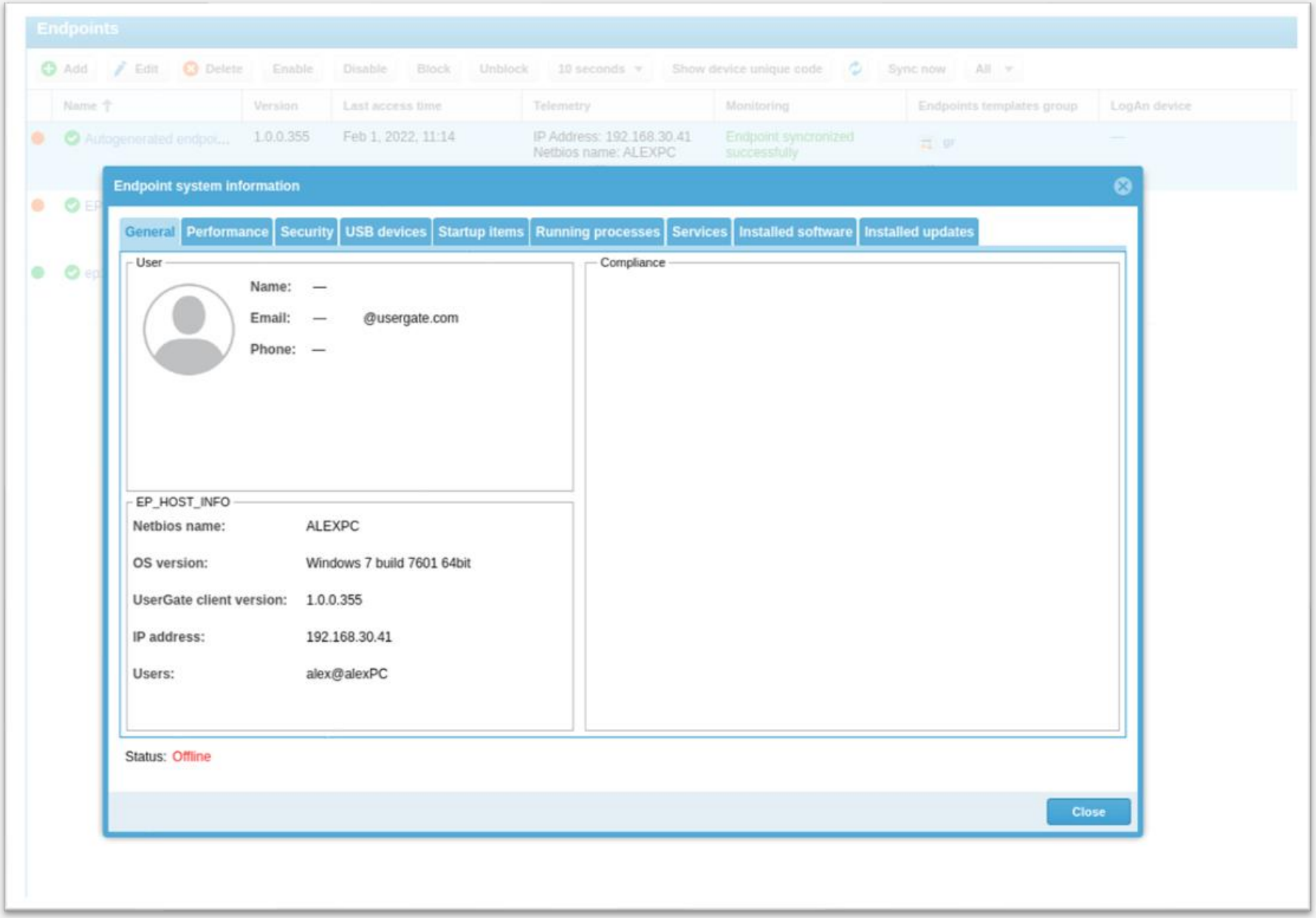
ПЕРИМЕТР РАСТЯГИВАЕТСЯ

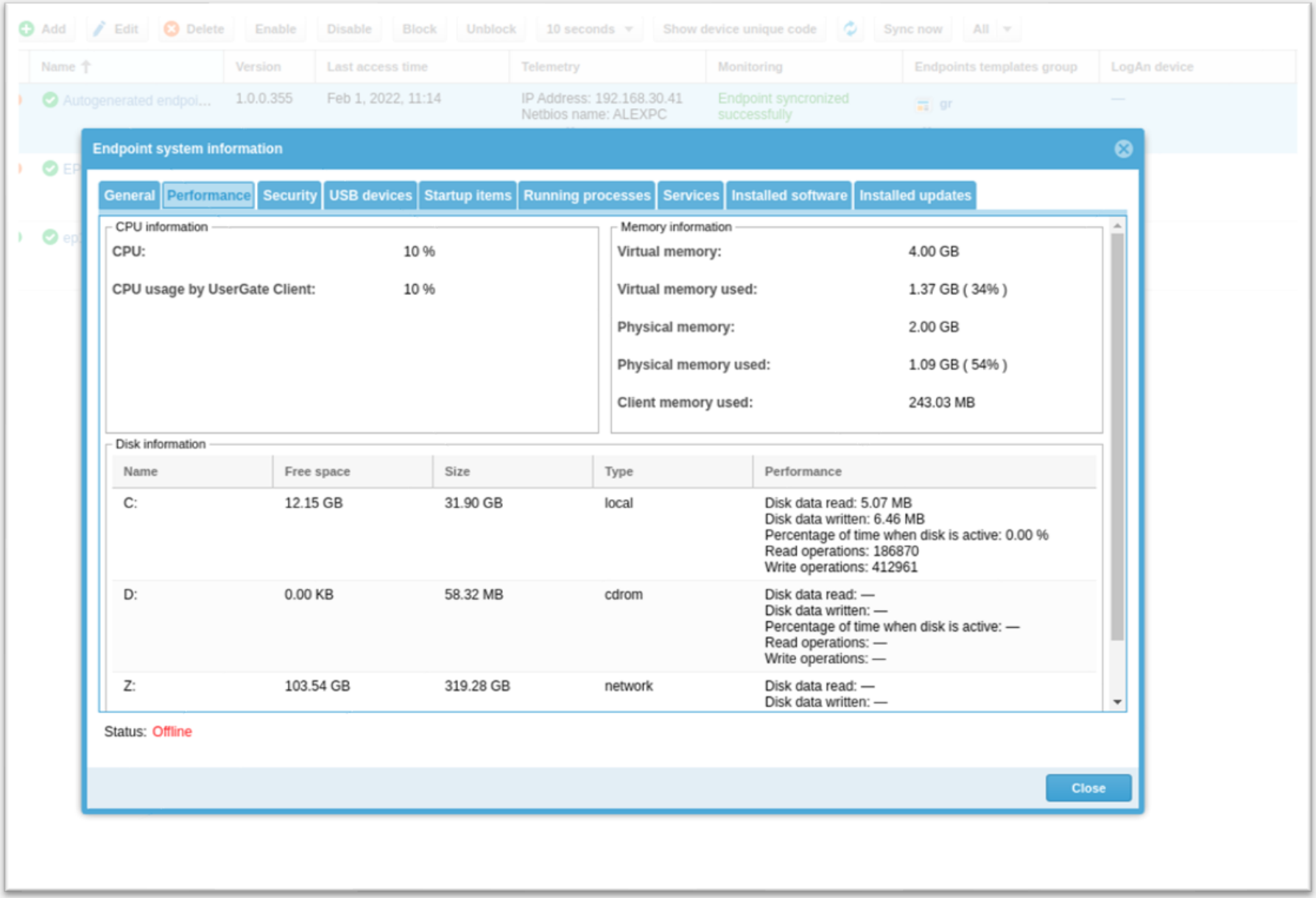
- Переход в облака – виртуальные решения и сервисы
- Безопасная публикация ресурсов
- Концепция нулевого доверия

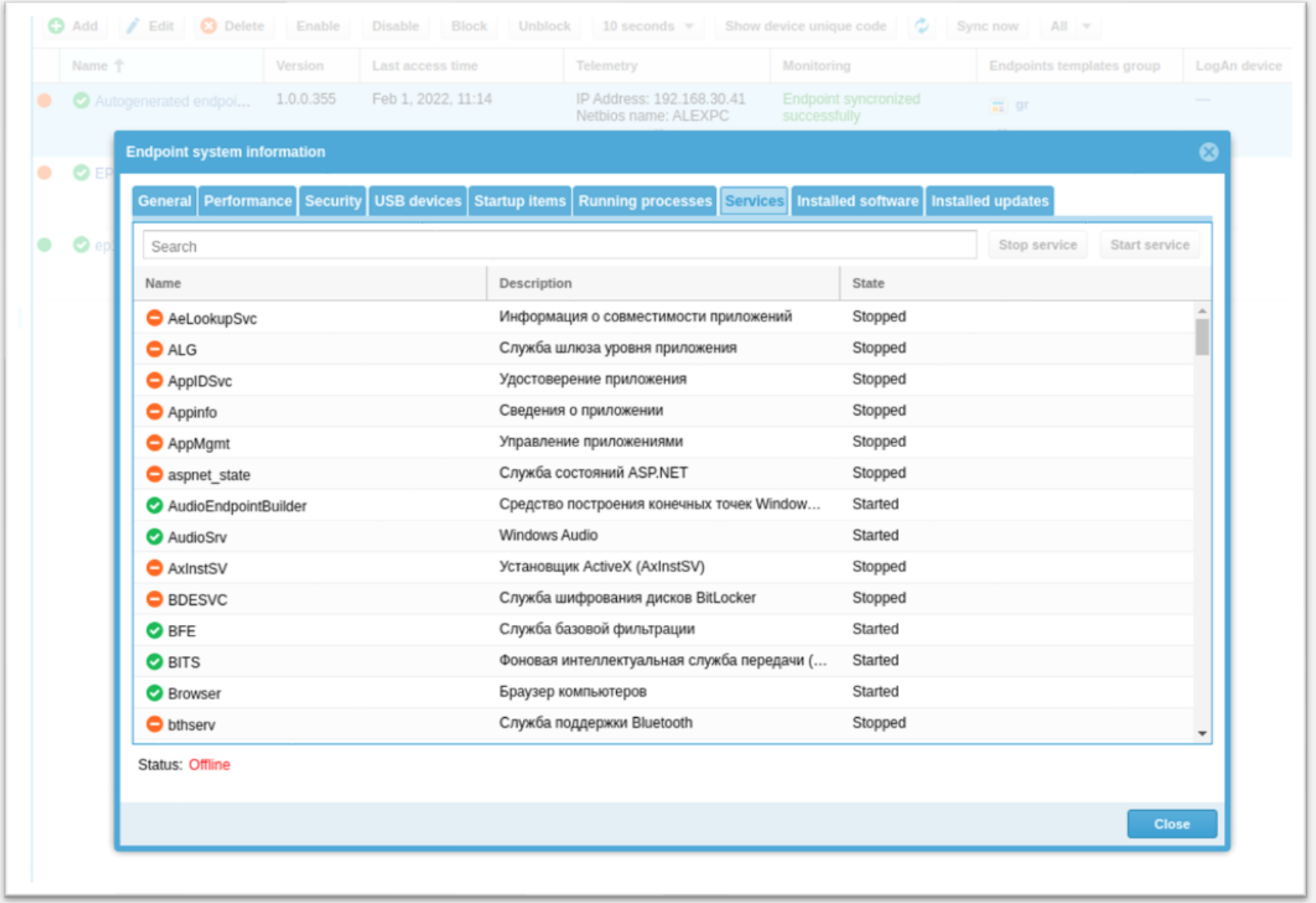
- Дополнительная видимость
- Инструмент обнаружения сложных угроз: **IoC** и **IoA**
- Углубленная информация
- Автоматизация процессов безопасности
- Межсетевой экран уровня хоста
- Дополнительный уровень аутентификации
- VPN-клиент для организации безопасного удаленного доступа

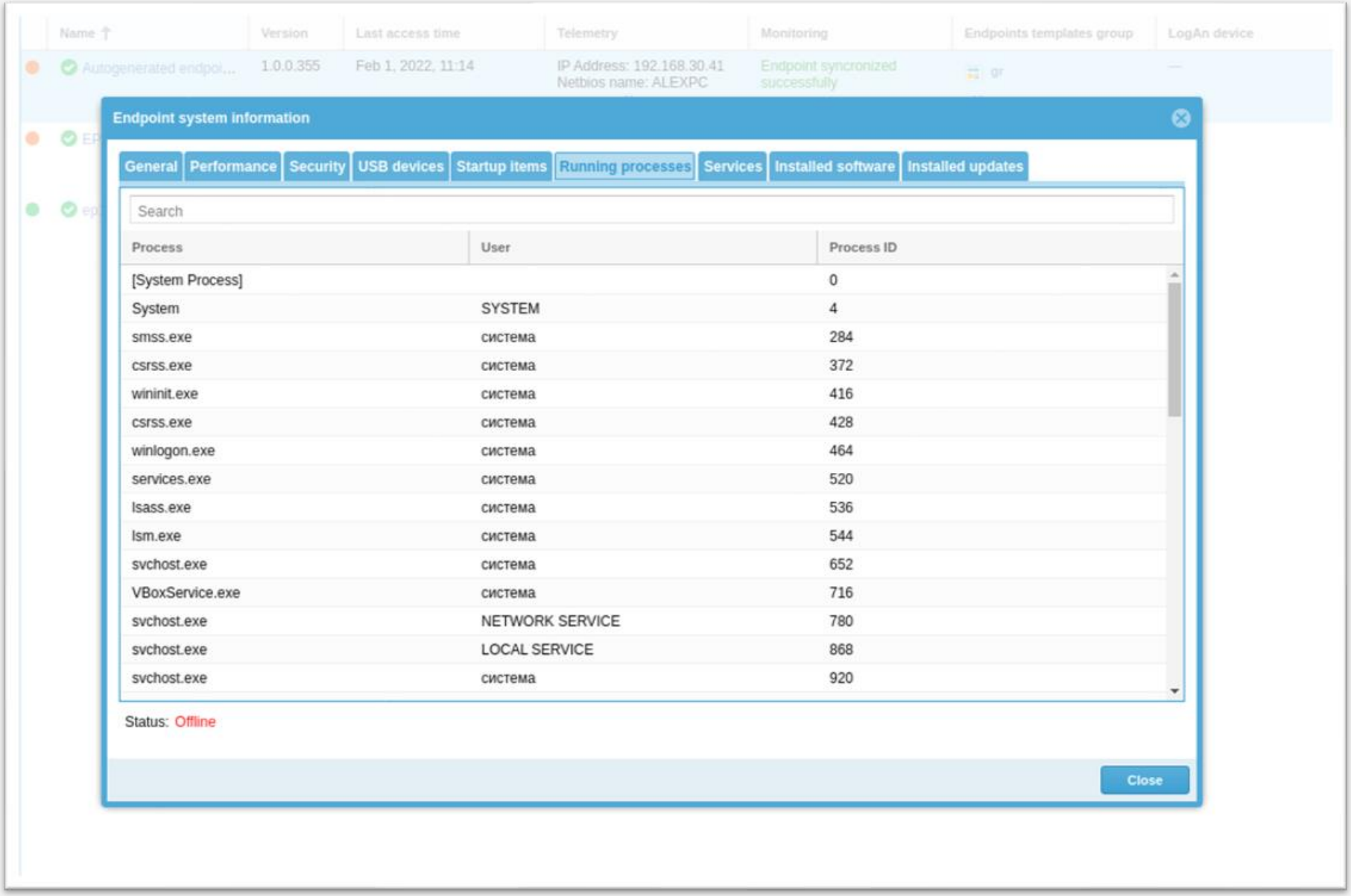



UserGate
Realm management | NGFW templates | Endpoints templates | LogAn templates | Logs and reports | Help | English | ex_admin
Central management console
General settings
Administrators
Auth servers
Auth profiles
Users catalogs
NGFW management
Templates
Template groups
Managed devices
Software updates
Libraries updates
Endpoints management
Templates
Templates groups
Endpoint codes
Endpoints
Software updates
Libraries updates
LogAn management
Templates
Template groups
LogAn devices
Software updates
Libraries updates
Endpoints
Add
Edit
Delete
Enable
Disable
Block
Unblock
10 seconds
Show device unique code
Sync now
All
Name
Version
Last access time
Telemetry
Monitoring
Endpoints templates group
LogAn device
Last successful sync time
Autogenerated endpoi...
1.0.0.355
Feb 1, 2022, 11:14
IP Address: 192.168.30.41
Netbios name: ALEXPC
More
Endpoint syncronized successfully
Endpoint system information...
gr
More
—
Sync mode: Auto sync
Feb 1, 2022, 11:14
EP2
1.0.0.355
Feb 1, 2022, 03:40
IP Address: 192.168.30.41
Netbios name: ALEXPC
More
Endpoint syncronized successfully
Endpoint system information...
gr
More
—
Sync mode: Auto sync
Feb 1, 2022, 03:40
ep1
1.0.0.355
Feb 1, 2022, 11:19
IP Address: 192.168.44.62
Netbios name: WIN8PC
More
Endpoint syncronized successfully
Endpoint system information...
gr
More
—
Sync mode: Auto sync
Feb 1, 2022, 11:19
Page 1 of 1
Find:


Endpoints
Add
Edit
Delete
Enable
Disable
Block
Unblock
10 seconds
Show device unique code
Sync now
All
Name
Version
Last access time
Telemetry
Monitoring
Endpoints templates group
LogAn device
1.0.0.355
Feb 1, 2022, 11:14
IP Address: 192.168.30.41
Netbios name: ALEXPC
Endpoint syncronized successfully
Endpoint system information
General
Performance
Security
USB devices
Startup items
Running processes
Services
Installed software
Installed updates
User
Name: —
Email: — @usergate.com
Phone: —
Compliance
EP_HOST_INFO
Netbios name: ALEXPC
OS version: Windows 7 build 7601 64bit
UserGate client version: 1.0.0.355
IP address: 192.168.30.41
Users: alex@alexPC
Status: Offline
Close


Add
Edit
Delete
Enable
Disable
Block
Unblock
10 seconds
Show device unique code
Sync now
All
Name
Version
Last access time
Telemetry
Monitoring
Endpoints templates group
LogAn device
Autogenerated endpoi...
1.0.0.355
Feb 1, 2022, 11:14
IP Address: 192.168.30.41
Netbios name: ALEXPC
Endpoint syncronized successfully
gr
Endpoint system information
General
Performance
Security
USB devices
Startup items
Running processes
Services
Installed software
Installed updates
CPU information
CPU:
10 %
CPU usage by UserGate Client:
10 %
Memory information
Virtual memory:
4.00 GB
Virtual memory used:
1.37 GB (34%)
Physical memory:
2.00 GB
Physical memory used:
1.09 GB (54%)
Client memory used:
243.03 MB
Disk information
Name
Free space
Size
Type
Performance
C:
12.15 GB
31.90 GB
local
Disk data read: 5.07 MB
Disk data written: 6.46 MB
Percentage of time when disk is active: 0.00 %
Read operations: 186870
Write operations: 412961
D:
0.00 KB
58.32 MB
cdrom
Disk data read: —
Disk data written: —
Percentage of time when disk is active: —
Read operations: —
Write operations: —
Z:
103.54 GB
319.28 GB
network
Disk data read: —
Disk data written: —
Status: Offline
Close


Add
Edit
Delete
Enable
Disable
Block
Unblock
10 seconds
Show device unique code
Sync now
All
Name
Version
Last access time
Telemetry
Monitoring
Endpoints templates group
LogAn device
Autogenerated endpoi...
1.0.0.355
Feb 1, 2022, 11:14
IP Address: 192.168.30.41
Netbios name: ALEXPC
Endpoint syncronized successfully
gr
Endpoint system information
General
Performance
Security
USB devices
Startup items
Running processes
Services
Installed software
Installed updates
Search
Stop service
Start service
Name
Description
State
AeLookupSvc
Информация о совместимости приложений
Stopped
ALG
Служба шлюза уровня приложения
Stopped
AppIDSvc
Удостоверение приложения
Stopped
Appinfo
Сведения о приложении
Stopped
AppMgmt
Управление приложениями
Stopped
aspnet_state
Служба состояний ASP.NET
Stopped
AudioEndpointBuilder
Средство построения конечных точек Window...
Started
AudioSrv
Windows Audio
Started
AxInstSV
Установщик ActiveX (AxInstSV)
Stopped
BDESVC
Служба шифрования дисков BitLocker
Stopped
BFE
Служба базовой фильтрации
Started
BITS
Фоновая интеллектуальная служба передачи (...
Started
Browser
Браузер компьютеров
Started
bthserv
Служба поддержки Bluetooth
Stopped
Status: Offline
Close


Name
Version
Last access time
Telemetry
Monitoring
Endpoints templates group
LogAn device
Autogenerated endpoi...
1.0.0.355
Feb 1, 2022, 11:14
IP Address: 192.168.30.41
Netbios name: ALEXPC
Endpoint syncronized successfully
Endpoint system information
General
Performance
Security
USB devices
Startup items
Running processes
Services
Installed software
Installed updates
Search
Process
User
Process ID
[System Process] 0
System SYSTEM 4
smss.exe система 284
csrss.exe система 372
wininit.exe система 416
csrss.exe система 428
winlogon.exe система 464
services.exe система 520
lsass.exe система 536
lsm.exe система 544
svchost.exe система 652
VBoxService.exe система 716
svchost.exe NETWORK SERVICE 780
svchost.exe LOCAL SERVICE 868
svchost.exe система 920
Status: Offline
Close

UserGate

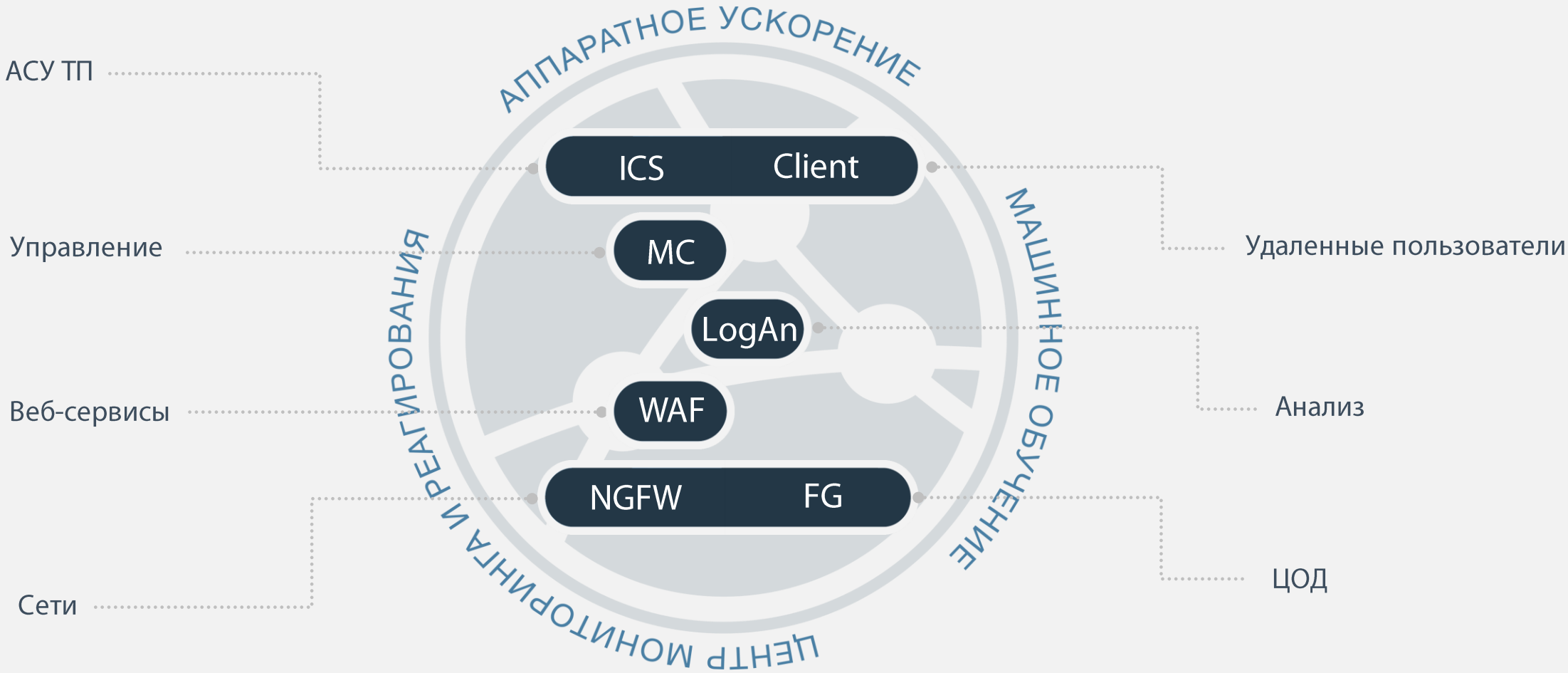
ПРОСЛОЙКА МЕЖДУ КРЕСЛОМ И АРМ

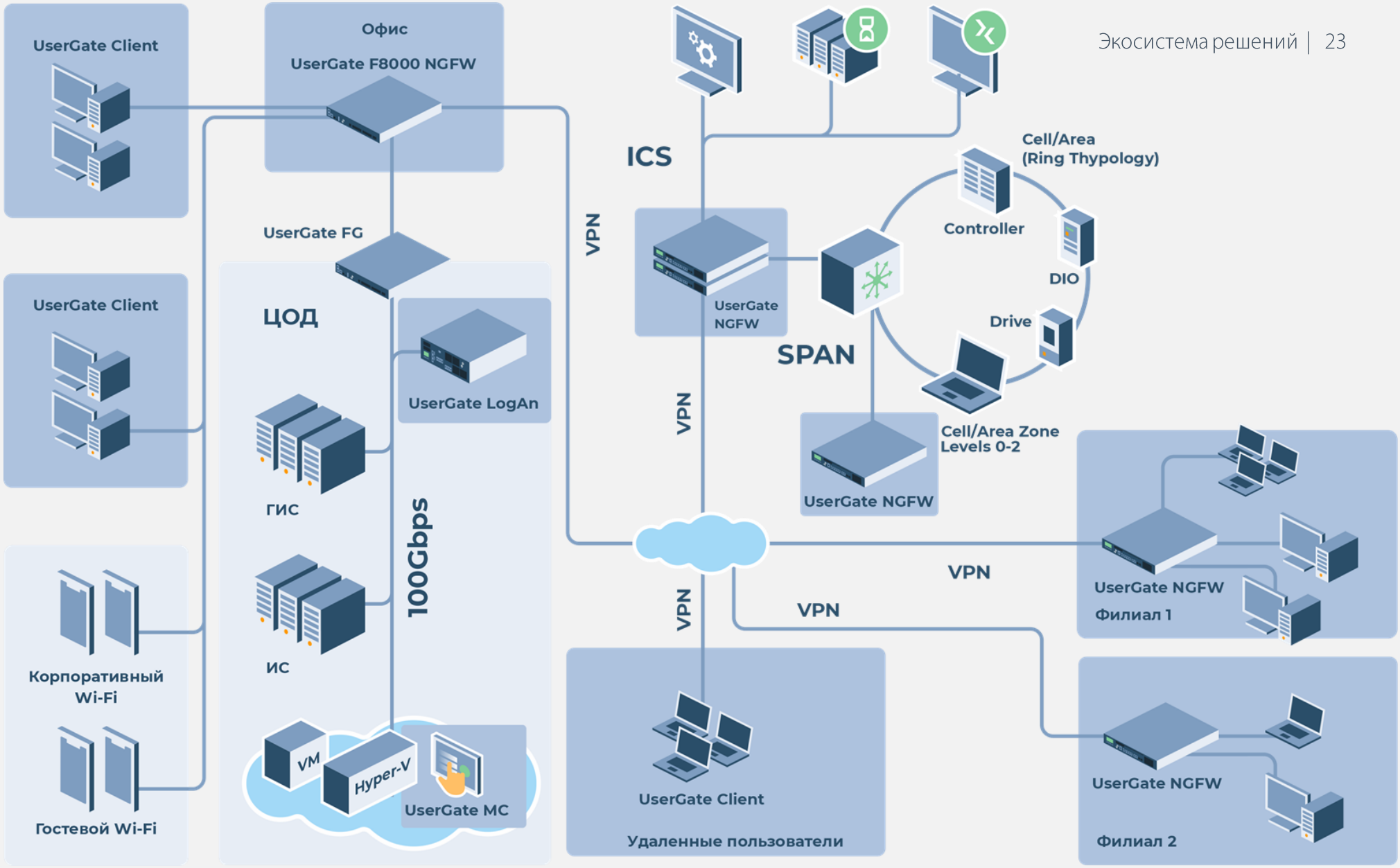
- Выстроенная политика доступа
- Гибкая фильтрация контента
- И еще раз про SSL


http
https

UserGate

USERGATE SUMMA


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


UserGate Client
Офис
UserGate F8000 NGFW
UserGate FG
UserGate Client
ЦОД
UserGate LogAn
ГИС
ИС
100Gbps
Корпоративный Wi-Fi
Гостевой Wi-Fi
VM
Hyper-V
UserGate MC
VPN
ICS
UserGate NGFW
Cell/Area (Ring Thypology)
Controller
DIO
Drive
SPAN
Cell/Area Zone Levels 0-2
UserGate NGFW
VPN
VPN
VPN
VPN
UserGate NGFW
Филиал 1
UserGate Client
Удаленные пользователи
UserGate NGFW
Филиал 2

UserGate

Virtual Appliance

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

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»

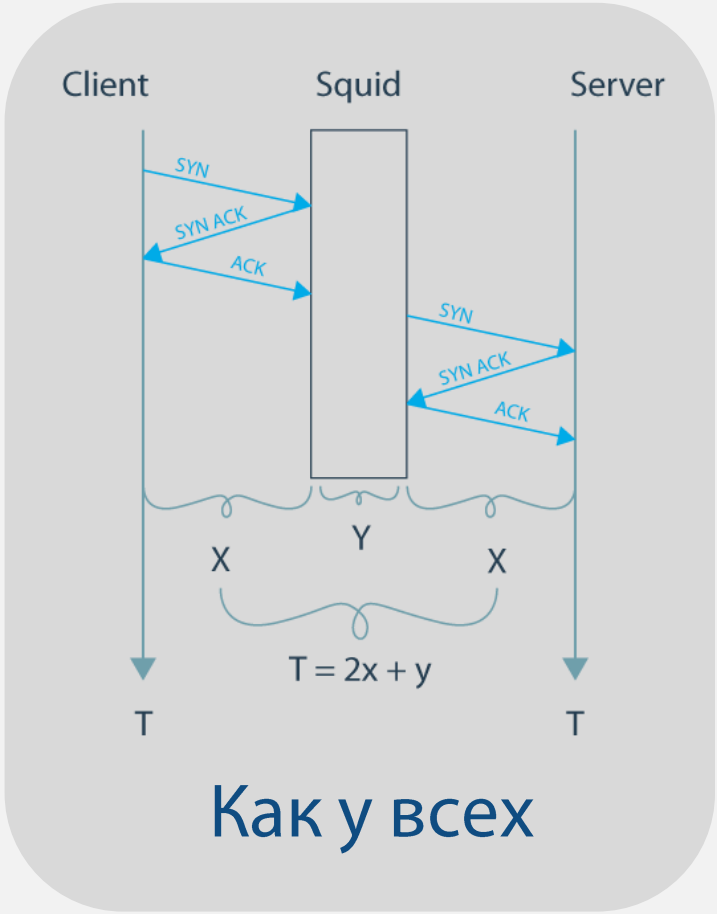
Уровень доверия 4:

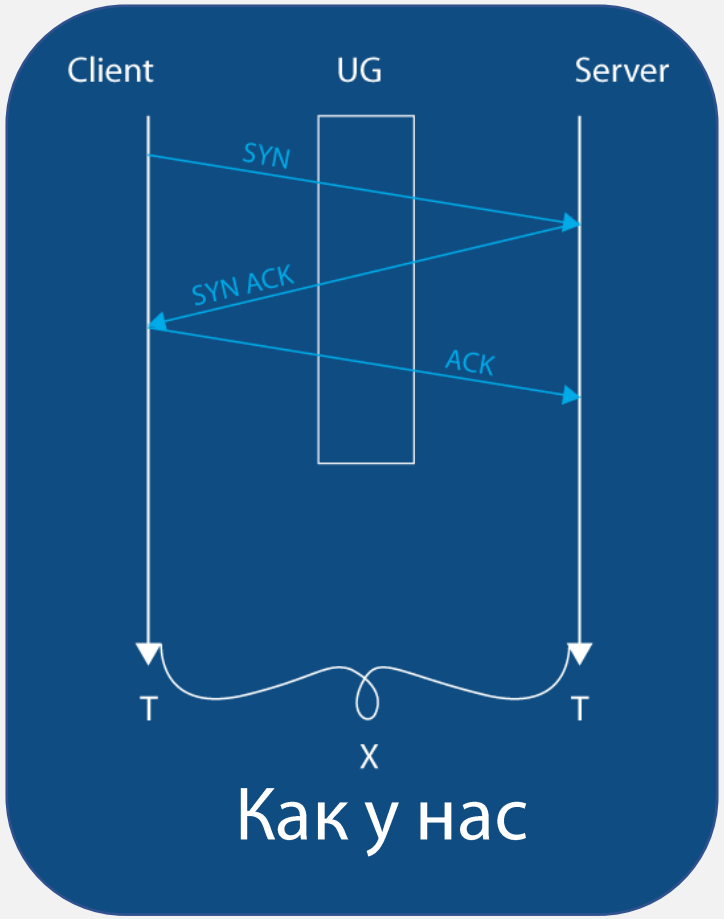
- Классы защиты СЗИ 4;
- ЗО КИИ 1 категории;
- ГИС 1 класса;
- АСУТП 1 класса;
- ИСПДн 1 уровня;
- ИСОП II класса

UserGate – самое **технологичное** решение **на российском рынке** сетевой безопасности

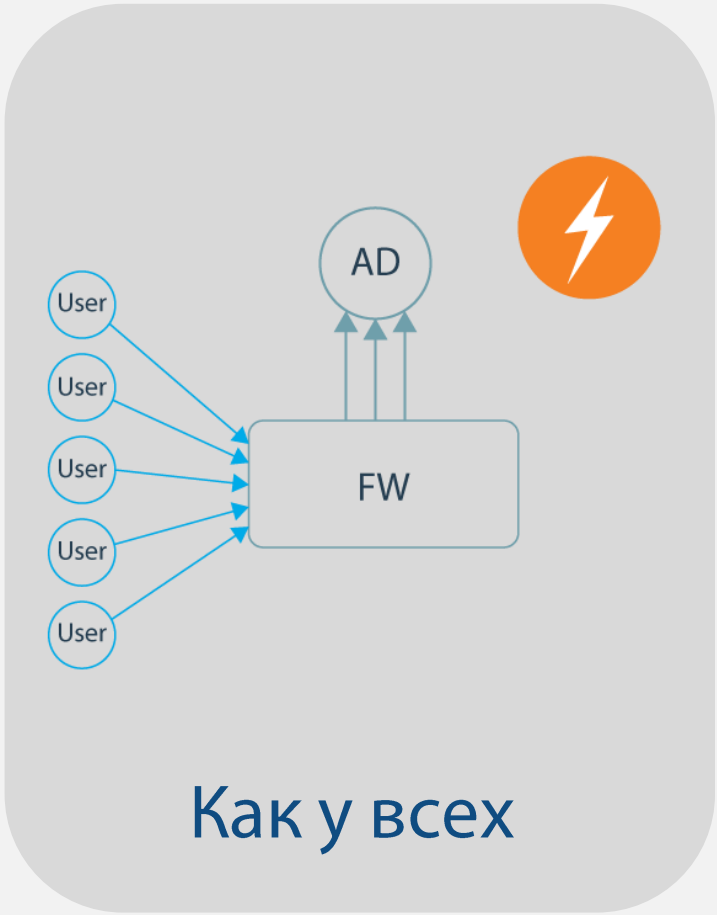
Фазовый обход правил

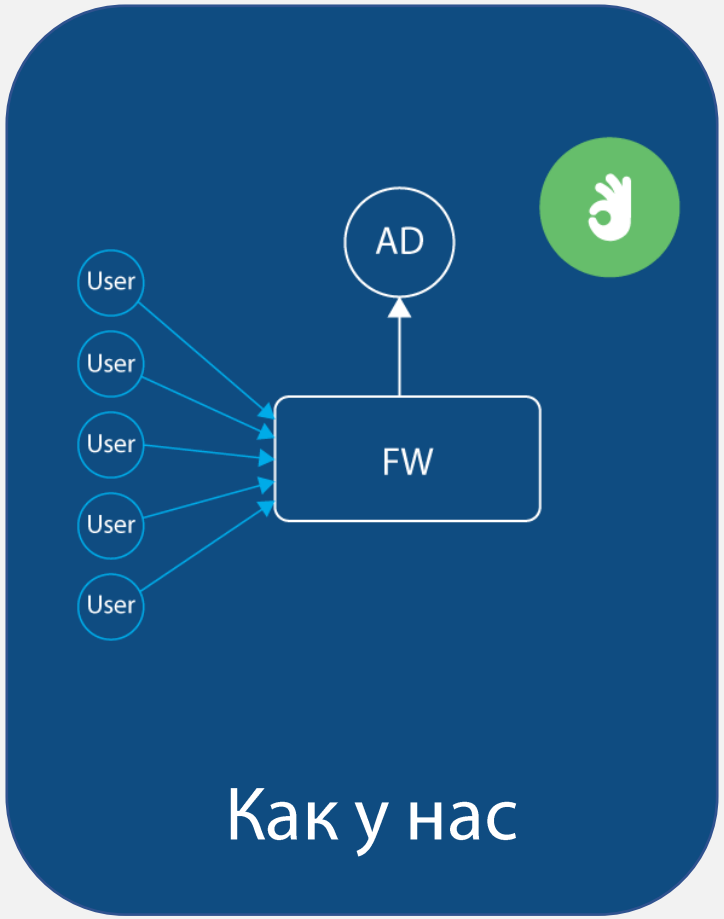
Контроль сетевого соединения





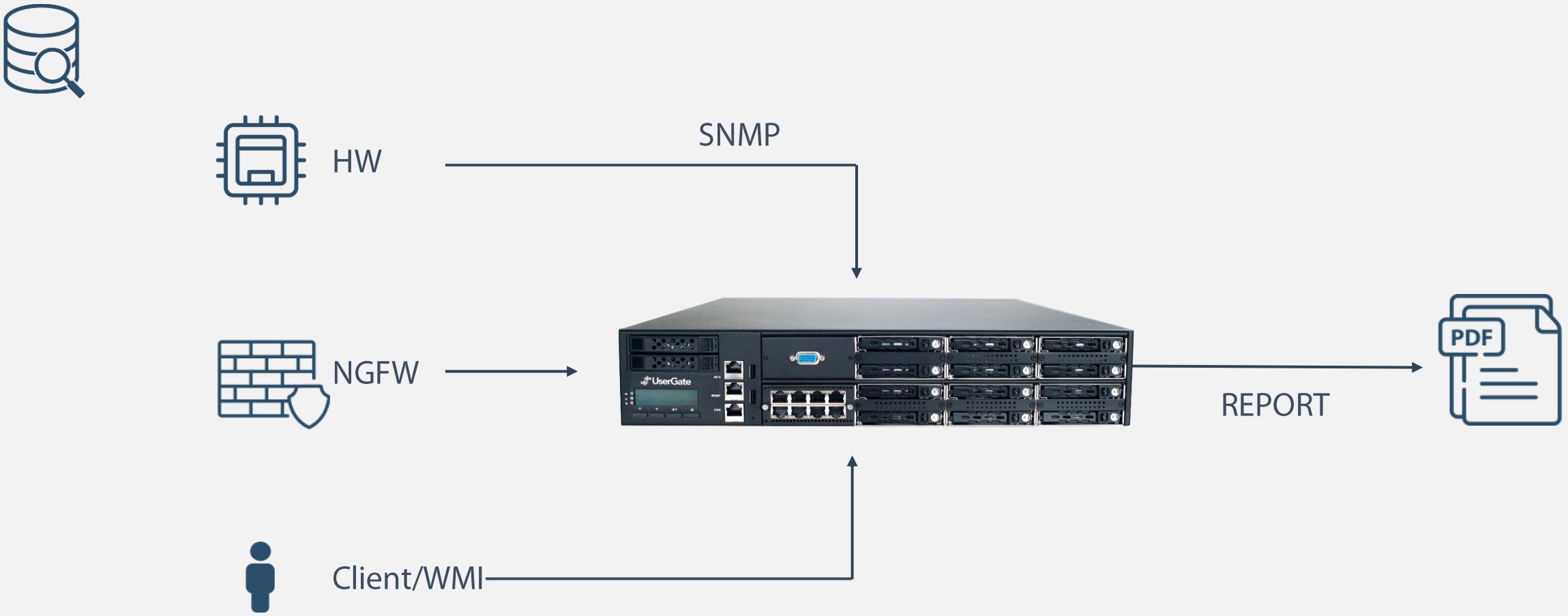
Авторизация пользователей

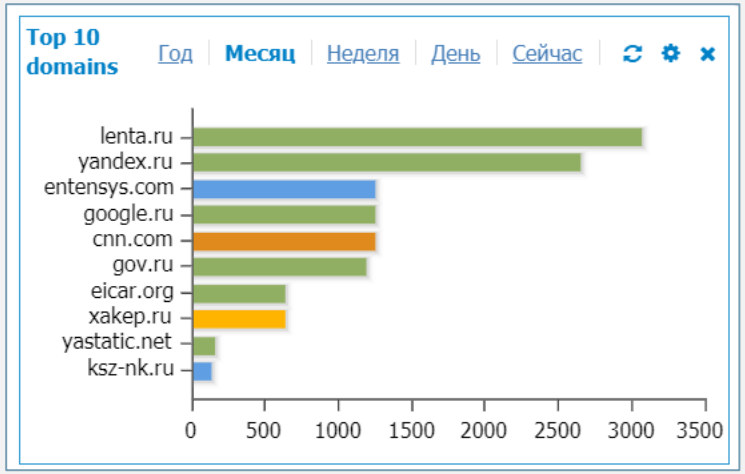




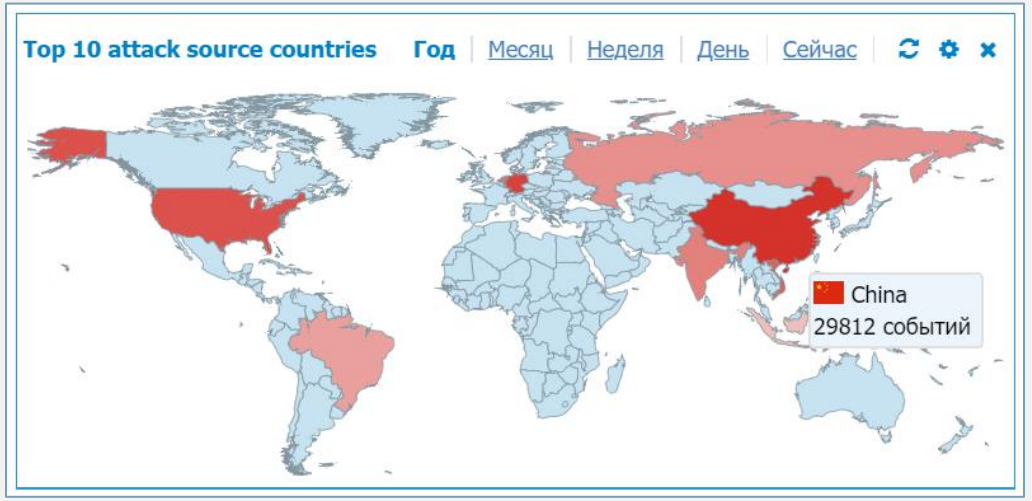
UserGate

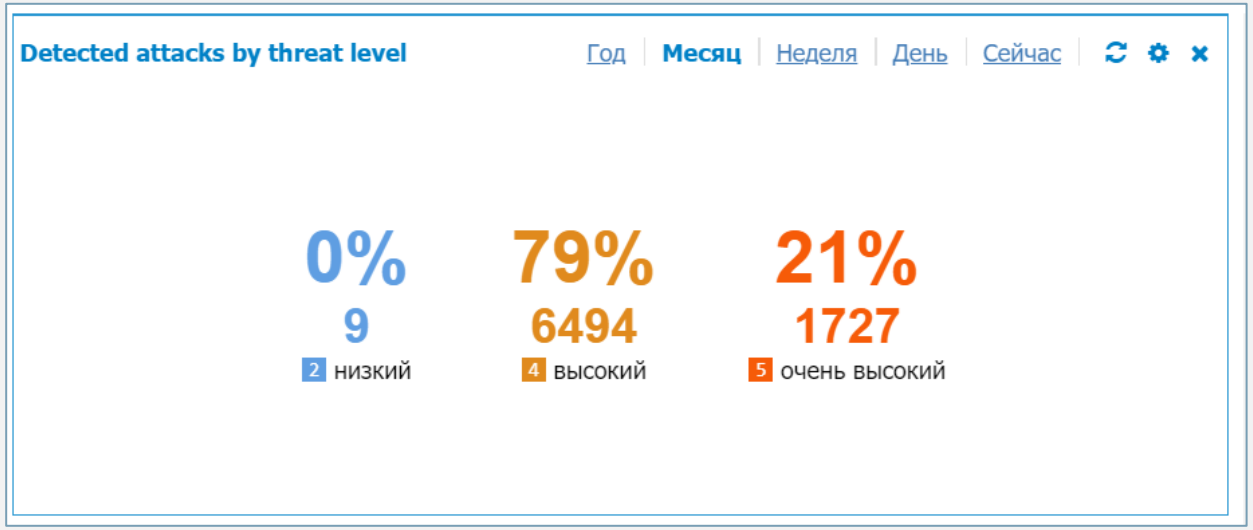
УПРАВЛЕНИЕ И АНАЛИЗ

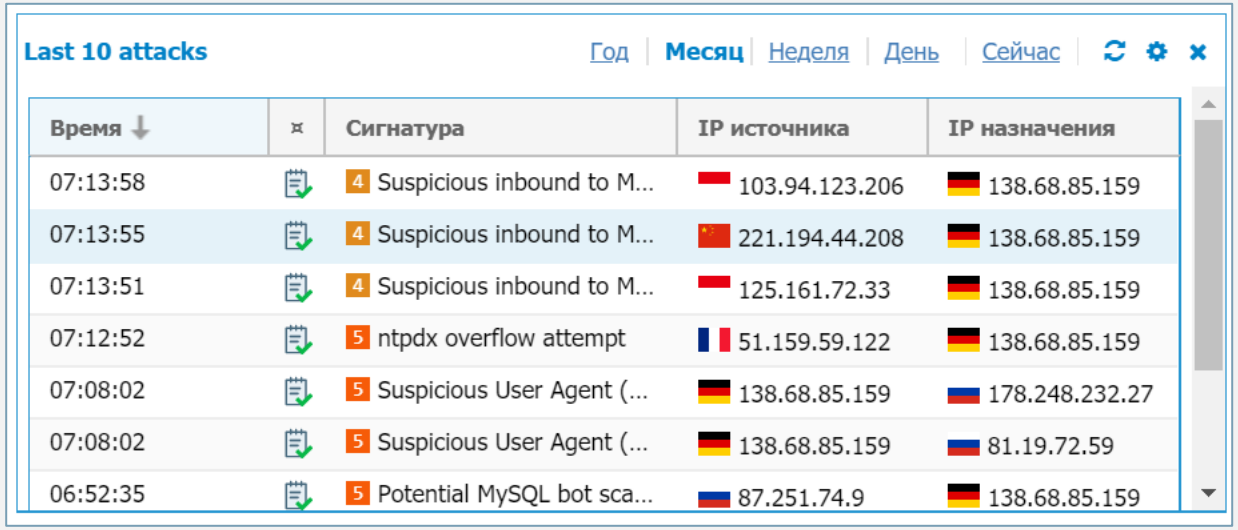

HW
SNMP
NGFW
REPORT
PDF
Client/WMI

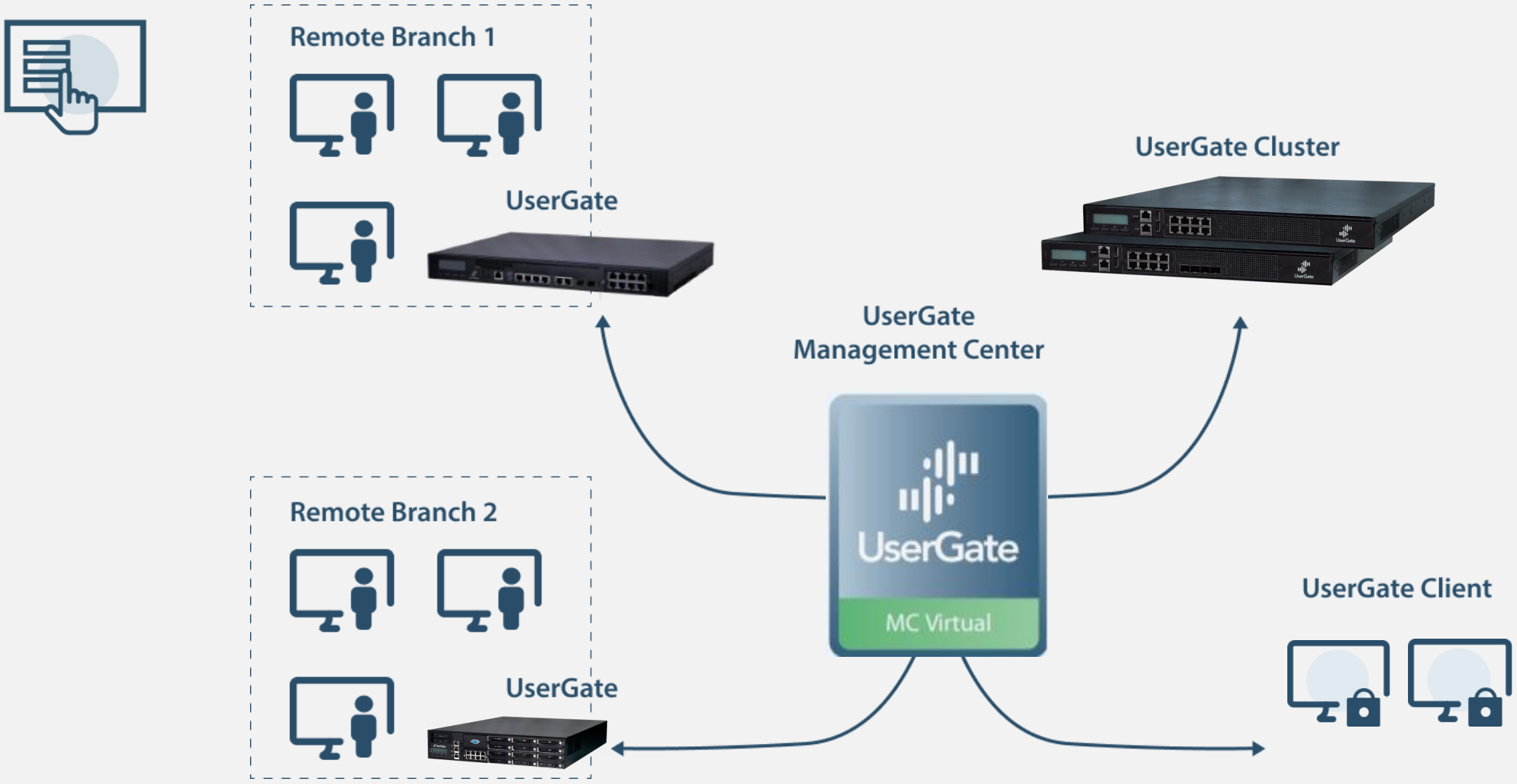

Top 10 domains
Год
Месяц
Неделя
День
Сейчас
lenta.ru
yandex.ru
entensys.com
google.ru
cnn.com
gov.ru
eicar.org
xakep.ru
yastatic.net
ksz-nk.ru
0
500
1000
1500
2000
2500
3000
3500

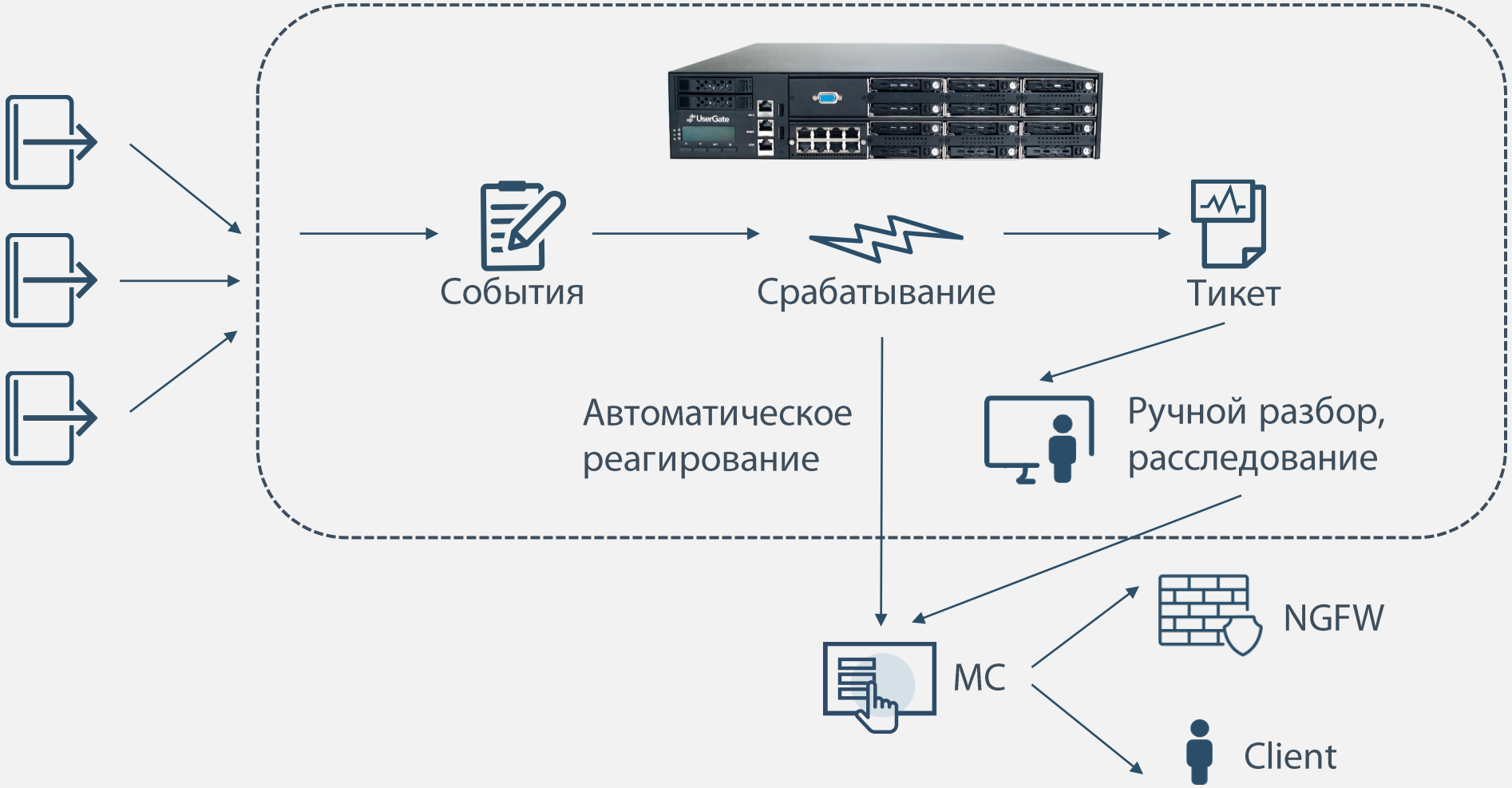

Top 10 categories
Год
Месяц
Неделя
День
Сейчас
Новости
Поисковые системы и порталы
Информационная безопасность
Бизнес
Потоковое мультимедиа и загрузки
Правительство
Развлечения
Компьютеры и технологии
Персональные сайты
0
10
20
30
40
50
60
70


Top 10 attack source countries
Год
Месяц
Неделя
День
Сейчас
China
29812 событий

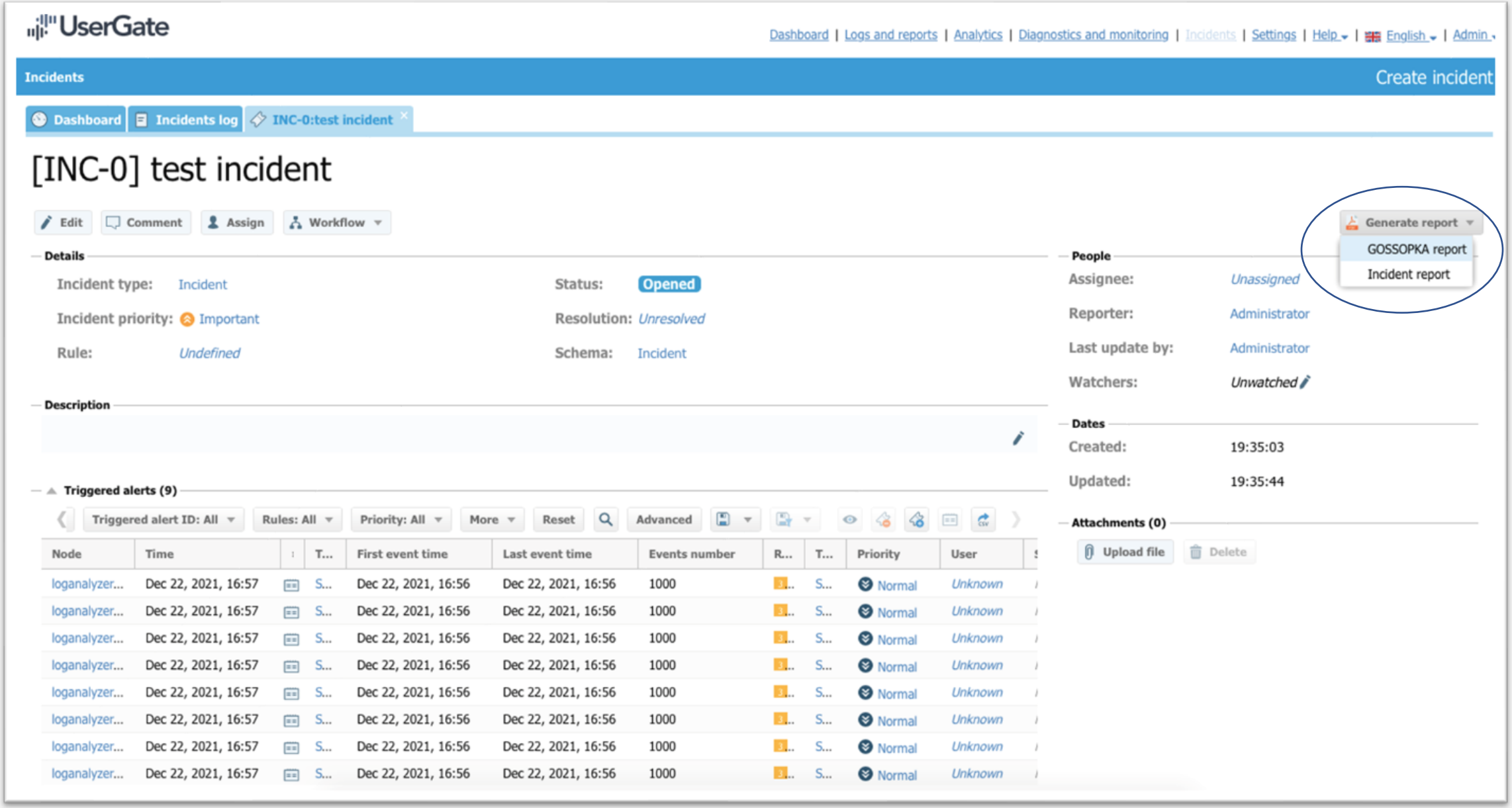

Detected attacks by threat level
Год
Месяц
Неделя
День
Сейчас
0%
9
2 низкий
79%
6494
4 высокий
21%
1727
5 очень высокий

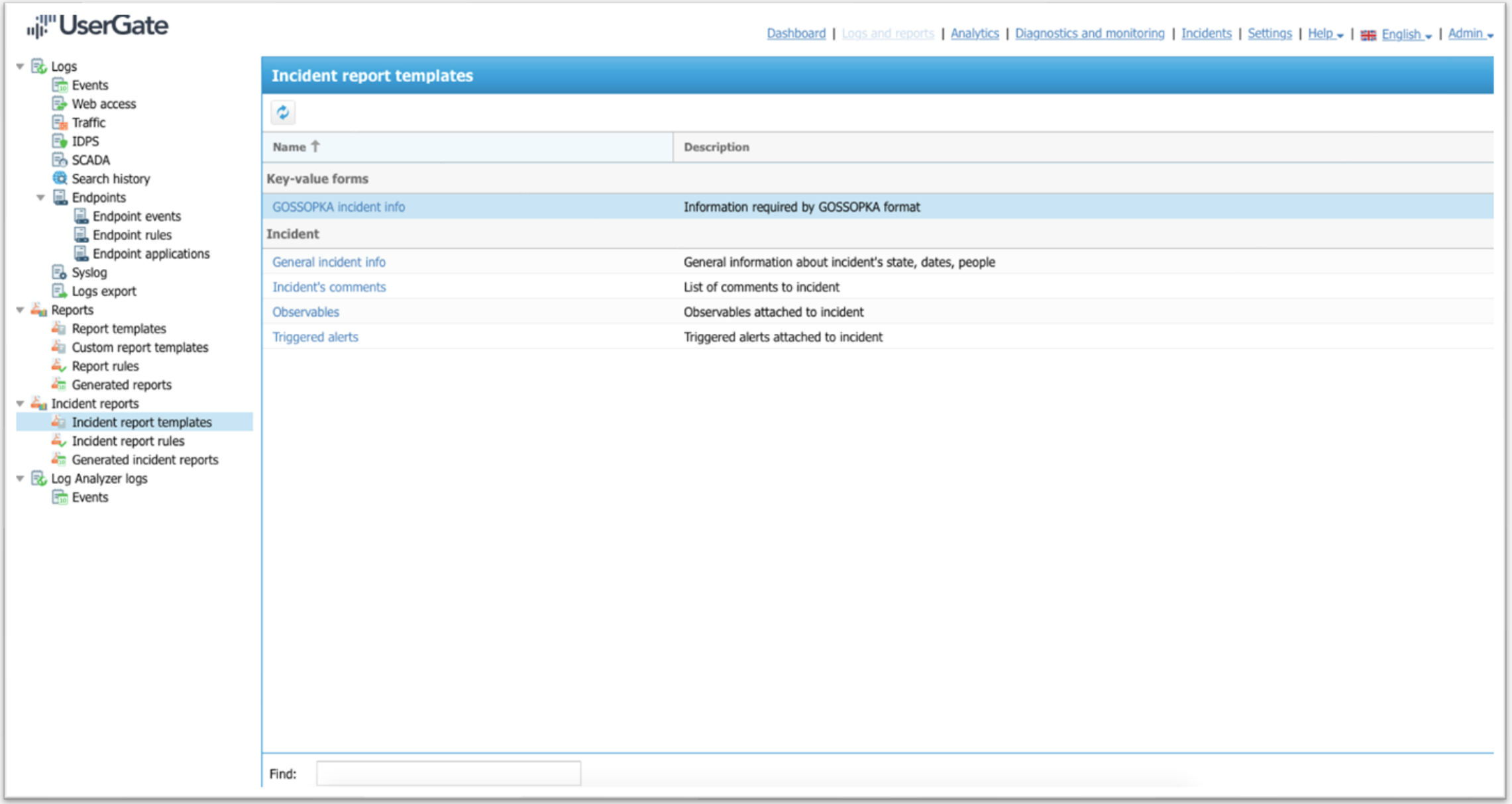

Last 10 attacks
Год
Месяц
Неделя
День
Сейчас
Время
Сигнатура
IP источника
IP назначения
07:13:58
4 Suspicious inbound to M...
103.94.123.206
138.68.85.159
07:13:55
4 Suspicious inbound to M...
221.194.44.208
138.68.85.159
07:13:51
4 Suspicious inbound to M...
125.161.72.33
138.68.85.159
07:12:52
5 ntpdx 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


Remote Branch 1
UserGate
UserGate Cluster
UserGate
Management Center
UserGate
MC Virtual
Remote Branch 2
UserGate
UserGate Client


События
Срабатывание
Тикет
Автоматическое
реагирование
Ручной разбор,
расследование
MC
NGFW
Client

LogAN + MC = SOAR


UserGate
Dashboard | Logs and reports | Analytics | Diagnostics and monitoring | Incidents | Settings | Help | English | Admin
Incidents
Create incident
Dashboard
Incidents log
INC-0:test incident
[INC-0] test incident
Edit
Comment
Assign
Workflow
Generate report
GOSSOPKA report
Incident report
Details
Incident type: Incident
Incident priority: Important
Rule: Undefined
Status: Opened
Resolution: Unresolved
Schema: Incident
People
Assignee: Unassigned
Reporter: Administrator
Last update by: Administrator
Watchers: Unwatched
Description
Dates
Created: 19:35:03
Updated: 19:35:44
Triggered alerts (9)
Triggered alert ID: All
Rules: All
Priority: All
More
Reset
Advanced
Attachments (0)
Upload file
Delete
Node
Time
T...
First event time
Last event time
Events number
R...
T...
Priority
User
loganalyzer...
Dec 22, 2021, 16:57
S...
Dec 22, 2021, 16:56
1000
Normal
Unknown

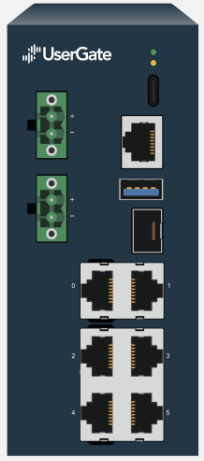

UserGate
Dashboard | Logs and reports | Analytics | Diagnostics and monitoring | Incidents | Settings | Help | English | Admin
Logs
Events
Web access
Traffic
IDPS
SCADA
Search history
Endpoints
Endpoint events
Endpoint rules
Endpoint applications
Syslog
Logs export
Reports
Report templates
Custom report templates
Report rules
Generated reports
Incident reports
Incident report templates
Incident report rules
Generated incident reports
Log Analyzer logs
Events
Incident report templates
Name
Description
Key-value forms
GOSSOPKA incident info
Information required by GOSSOPKA format
Incident
General incident info
General information about incident's state, dates, people
Incident's comments
List of comments to incident
Observables
Observables attached to incident
Triggered alerts
Triggered alerts attached to incident
Find:

UserGate

АППАРАТНЫЕ РАЗРАБОТКИ

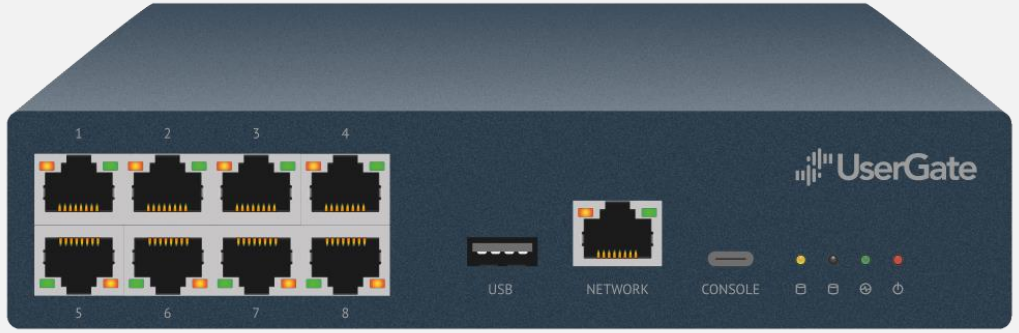
Собственные аппаратные платформы

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 до + 70 °C
- Крепление на DIN рейку

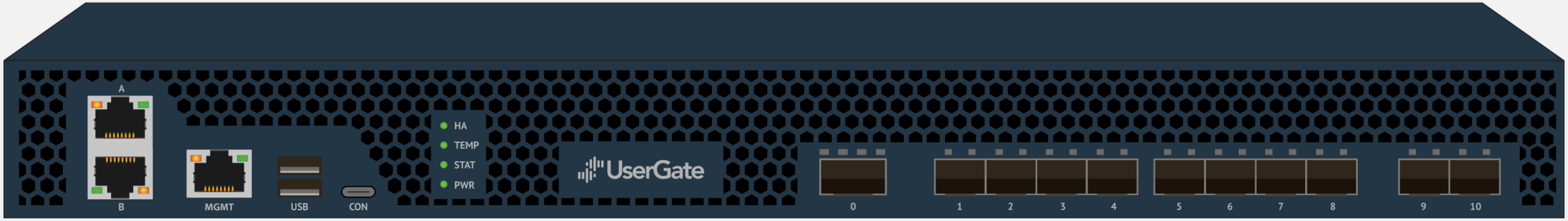
Модель C150



- FW до 2,5 Гб/с
- ARM 8 cores
- 8 портов 1GbE с поддержкой bypass
- Два блока питания
- От 0 до +70 °C

Новые платформы UserGate NGFW

UserGate FG



- Аппаратная обработка трафика на ПЛИС
- Производительность МЭ более 100+ Gbps пакеты 64 байта, трафик реальных приложений
- Производительность PPS ~ 120 Mpps
- Wire speed – производительность МЭ = скорости сетевого интерфейса
- Собственная разработка
- Доверие к ПАК из Минпромторга

Сетевые порты:

- 10 x 10 Gbps SFP+
- 1 x 100 Gbps QSFP28
- 2 x 1 Gbps BASE-T
- IPMI
- SSD: от 128 Гб
- RAM: от 64 Гб
- БП: 2 с горячей заменой

UserGate

СТАДИИ ПРИНЯТИЯ OPEN-SOURCE

1 стадия – «Для тех, кто вообще ничего не умеет»

- Готовые продукты:
  - pfSense
  - OPNSense
  - M0n0wall
  - IPCop
- Сколько их еще

2 стадия – «Для тех, кто сам научился собирать образы»

- Готовые компоненты:
  - Suricata
  - Snort
  - nDPI
  - Squid
  - OpenVPN
  - OpenSSL
  - И так далее

3 стадия – «Для профессионалов»

- Низкоуровневые библиотеки:
  - Iptables
    - Curl
    - Python
    - Apache
    - Bash
  - telnet-server
  - Сотни их

UserGate

ПРОСТО НАПОМНИТЬ

- Open Source – это хорошо, когда ты студент
- GeoIP ломает всю импортонезависимость
- Внимательно читайте лицензионное соглашение

McAfee SECURE

Check Point SOFTWARE TECHNOLOGIES LTD.

FORTINET

STONESOFT

paloalto NETWORKS

Microsoft Forefront

Barracuda

KerioControl

FORCEPOINT POWERED BY Raytheon

BlueCoat

UserGate

Спасибо за внимание

Александр Богданов

Партнерский отдел UserGate

abogdanov@usergate.com

+7 (800) 500 40 32 доб. 1033 | +7 (913) 792 61 48