UserGate

Удаленная работа

Иван Чернов
Менеджер по развитию

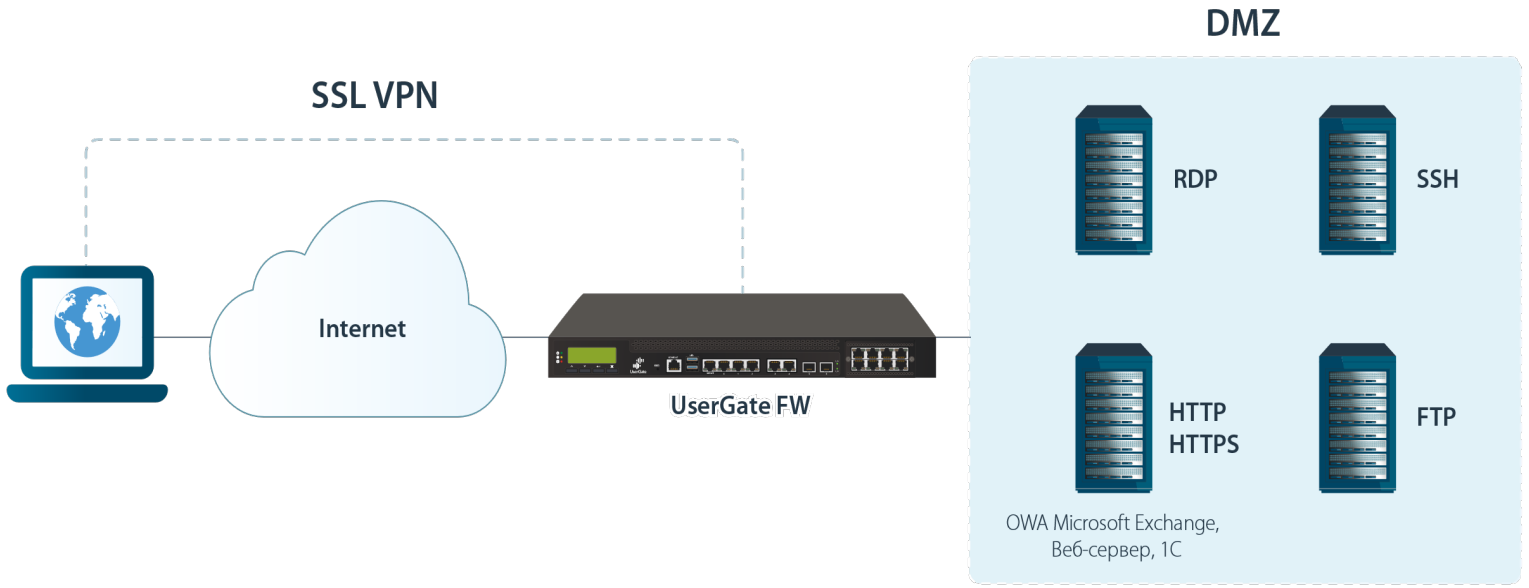
ichernov@usergate.com
+7 (983) 129-13-06

Проблематика

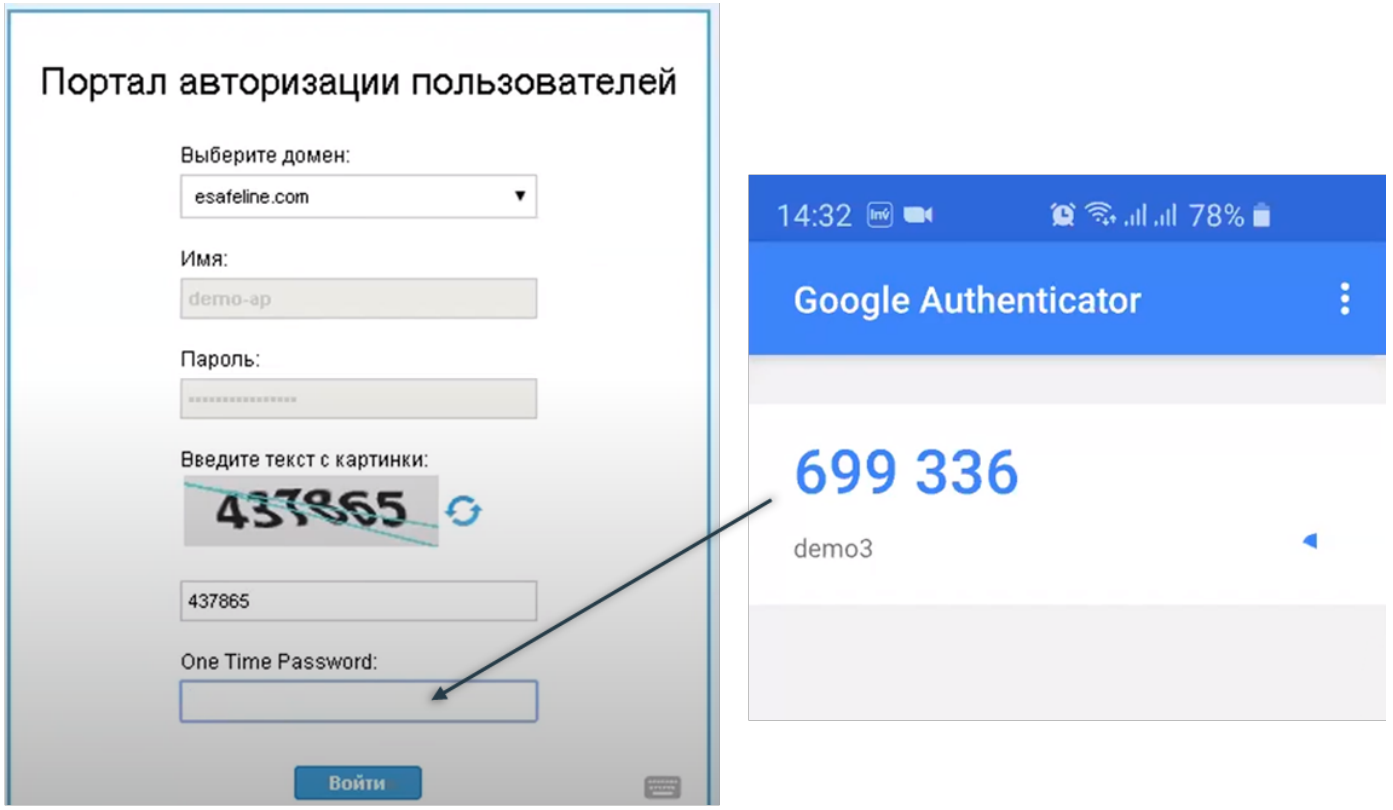
- Доверие к удаленному сотруднику
- Неподконтрольность удаленного устройства
- Источник угроз для корпоративной сети

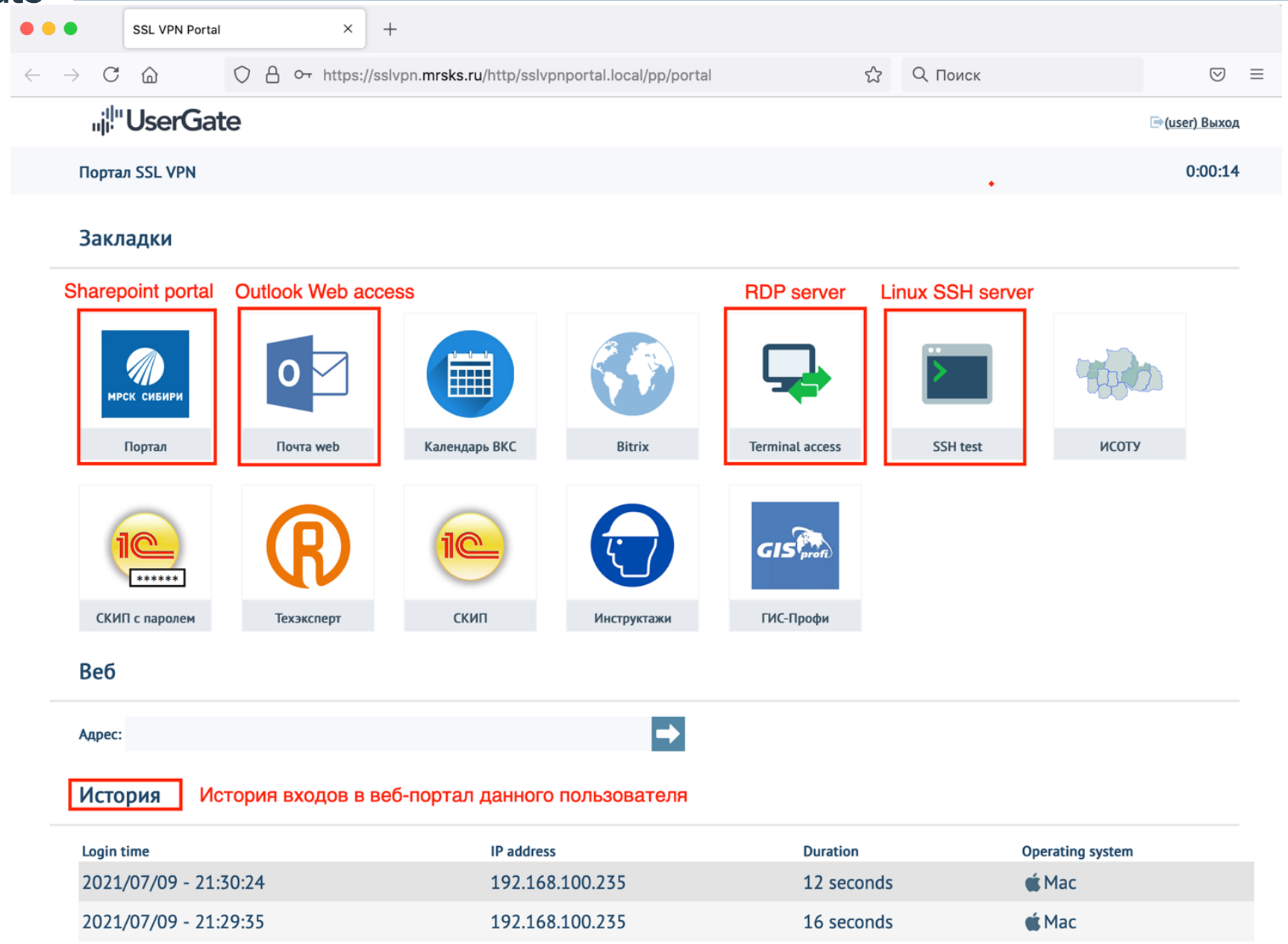
Решение

- Сегментирование зоны с удаленными сотрудниками
- Изоляция приложений на уровне сети
- Построение безопасного подключения


DMZ
SSL VPN
Internet
UserGate FW
RDP
SSH
HTTP
HTTPS
FTP
OWA Microsoft Exchange,
Веб-сервер, 1С

- MFA (TOTP, SMS, Email)
- Настройка политик доступа к отдельным сервисам по пользователям и группам
- Доступ через браузер
- SSO



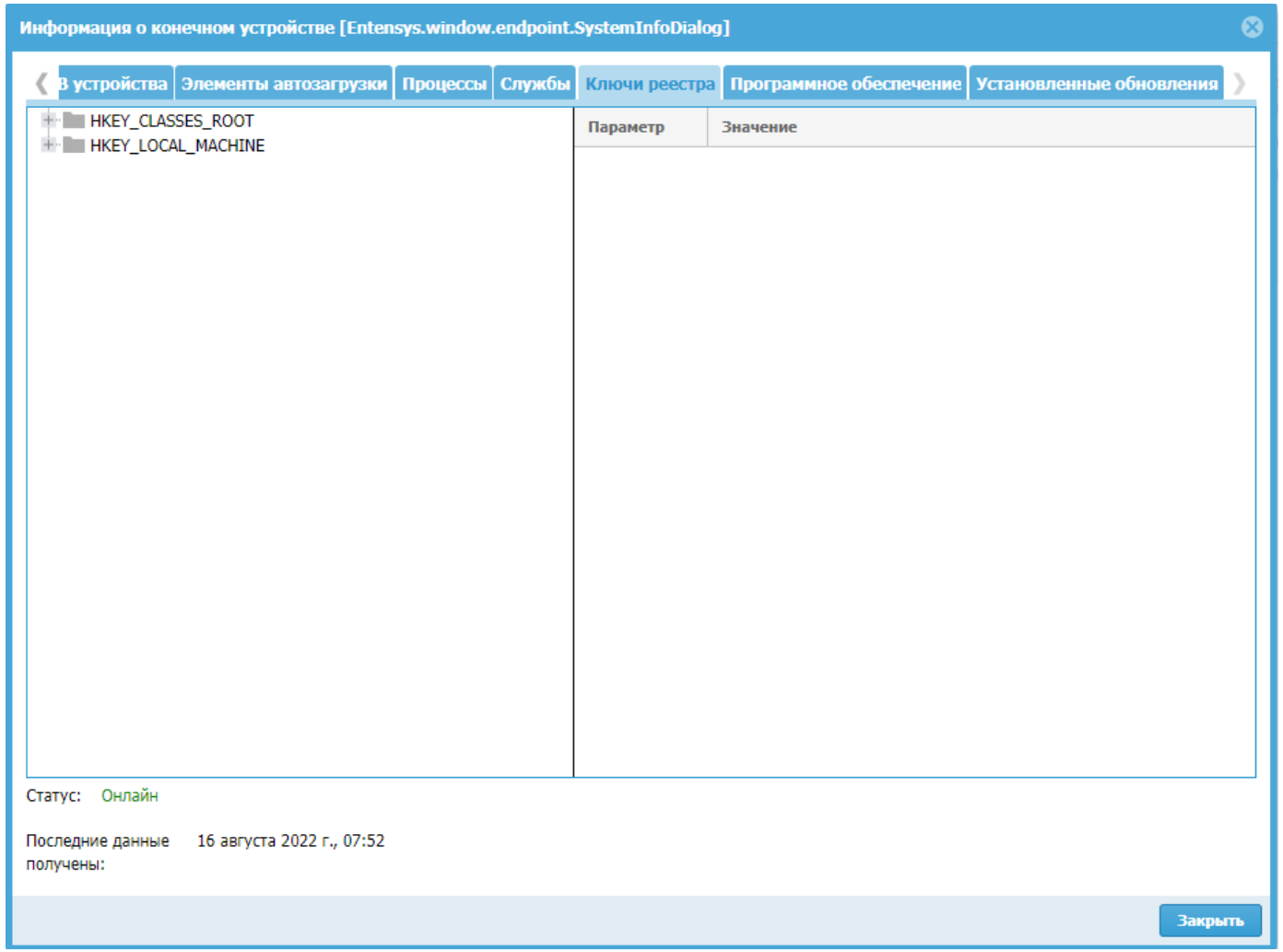

SSL VPN Portal
https://sslvpn.mrsks.ru/http/sslvpnportal.local/pp/portal
Поиск
UserGate
(user) Выход
Портал SSL VPN
0:00:14
Закладки
Sharepoint portal
Outlook Web access
RDP server
Linux SSH server
МРСК СИБИРИ
Портал
Почта web
Календарь ВКС
Bitrix
Terminal access
SSH test
ИСОТУ
******
СКИП с паролем
Техэксперт
СКИП
Инструктажи
GIS profi
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
Mac
2021/07/09 - 21:29:35
192.168.100.235
16 seconds
Mac

Безопасность удаленного сотрудника

UserGate Client - агент SUMMA:

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

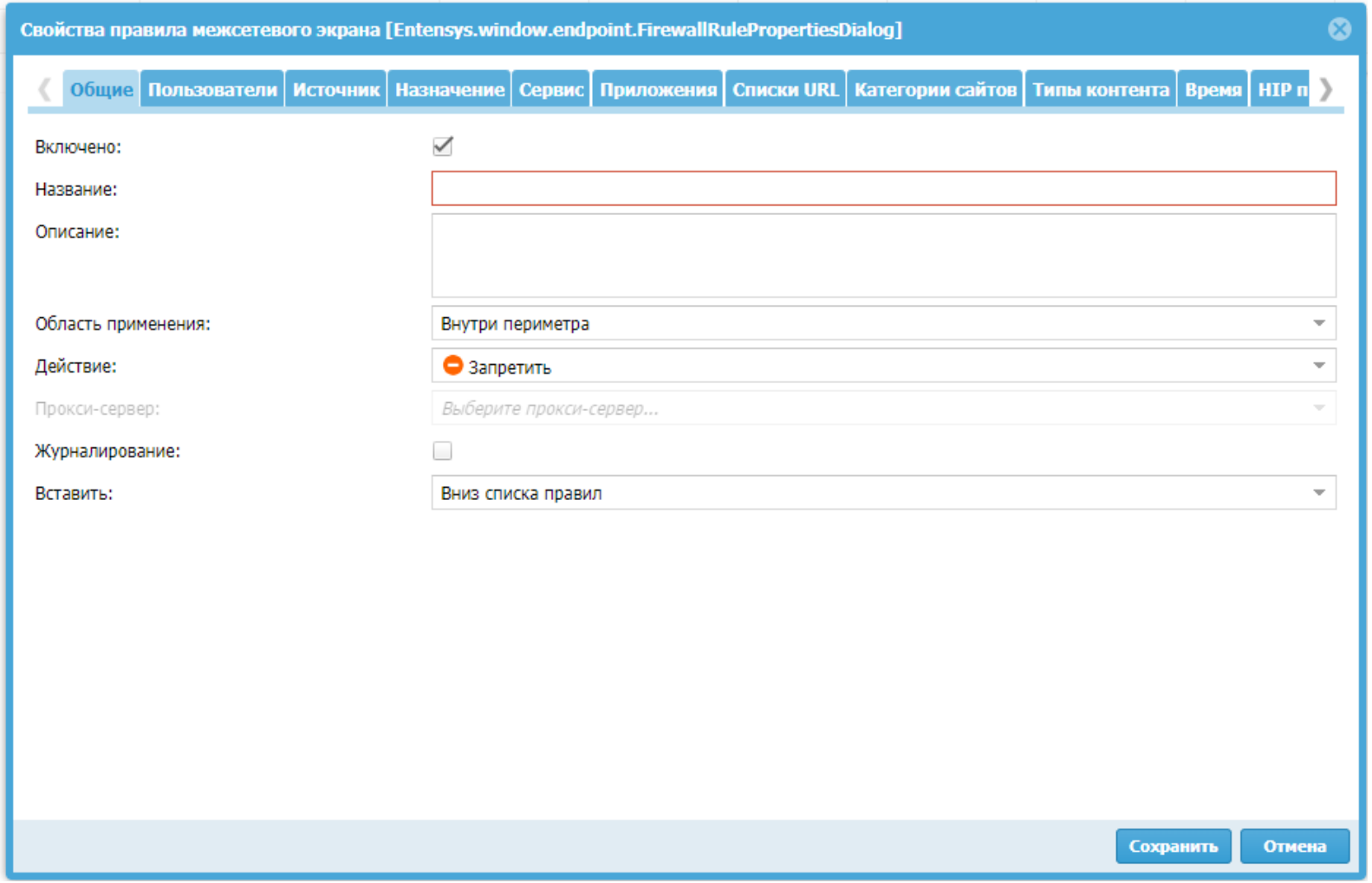
Сбор информации с устройства



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:

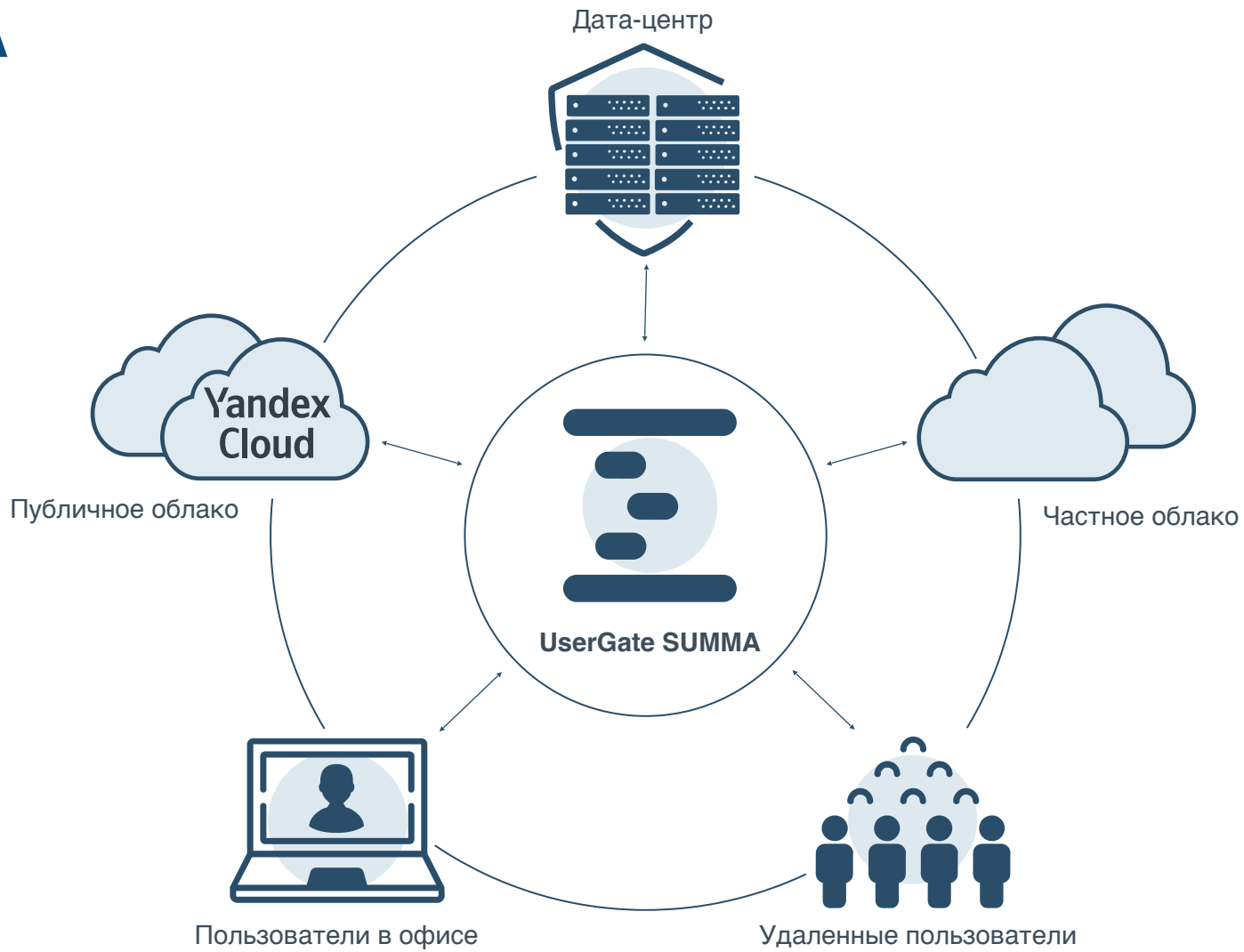
- IP-адреса;
- домены;
- имена и хеши файлов;
- ветки реестра.

В рамках UserGate SUMMA

EDR/XDR


Extended
Detection
Response
Сети
Облака
Устройства
UserGate Log Analyzer
SOC
Cloud Protection
UserGate Client
Proxy
NGFW
WAF

ZTNA


Дата-центр
Yandex Cloud
Публичное облако
Частное облако
UserGate SUMMA
Пользователи в офисе
Удаленные пользователи

UserGate

Спасибо за внимание!

Иван Чернов
Менеджер по развитию

ichernov@usergate.com
+7 (983) 129-13-06