EFROS
DEFENCE OPERATIONS

Доверять нельзя контролировать:

где поставить запятую
в современной сетевой безопасности?

Андрей Ситников
пресейл-инженер

GIS ГАЗИНФОРМ СЕРВИС

EFROS DEFENCE OPERATIONS

GIS ГАЗИНФОРМ СЕРВИС

О компании «Газинформсервис»

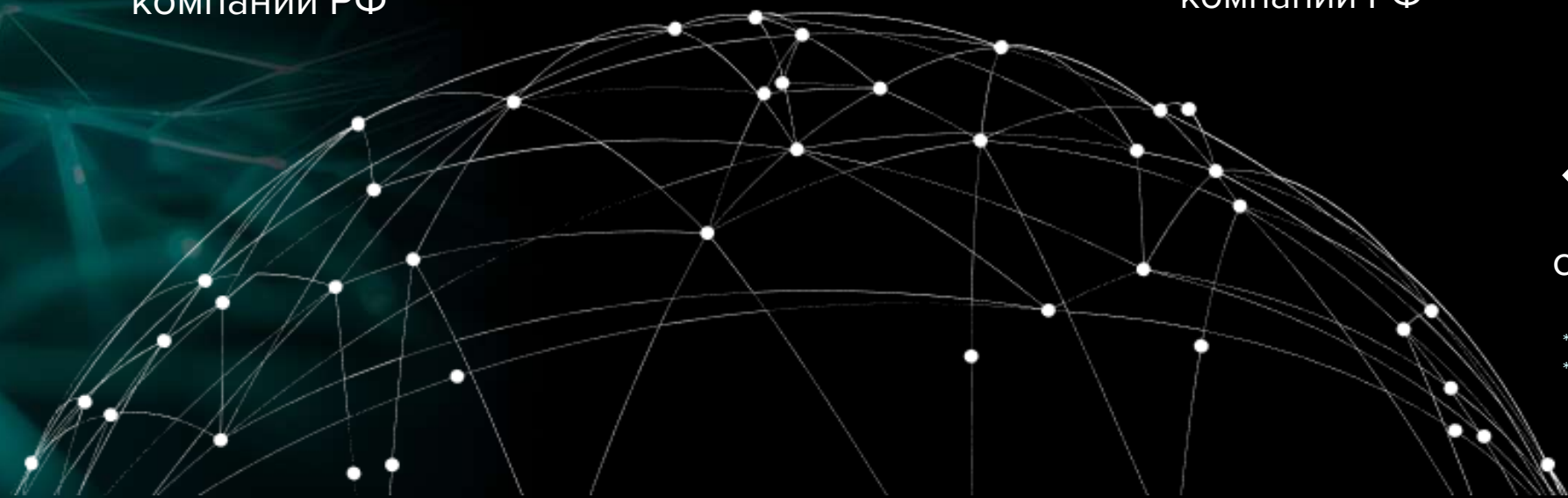
ООО «Газинформсервис» — один из крупнейших в России системных интеграторов в области безопасности и разработчиков средств защиты информации.

2
Среди ИБ-компаний РФ*

21
год

13
Среди ИТ-компаний РФ**

8
филиалов



1500
сотрудников

*по версии CNews
**в рейтинге TAdviser

www.gaz-is.ru

Актуальность проблематики контроля доступа в сеть

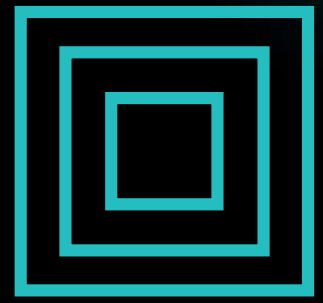
EFROS DEFENCE OPERATIONS

GIS ГАЗИНФОРМ СЕРВИС

Рост уровня киберугроз

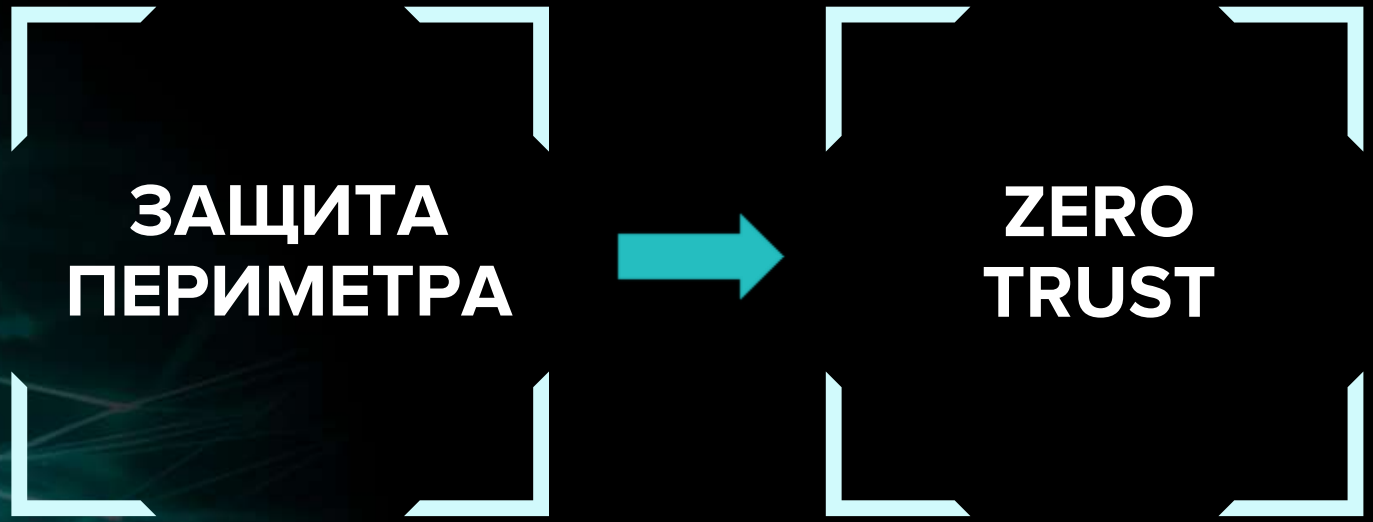
Рост числа пользователей и подключений

Рост числа устройств интернета вещей (принтеры, телефоны, видеокамеры, др.) **~ 80 млн** устройств в России (2024 г.)



РОСТ
ПОВЕРХНОСТИ
АТАК

Что такое «нулевое доверие»



ZTNA – стратегия / технология / фреймворк / архитектура

EFROS DEFENCE OPERATIONS

GIS ГАЗИНФОРМ СЕРВИС

Q.: С чего следует начать внедрение концепции ZTNA в компании?

A.: **Внедрение** стратегии ZTNA **начинают с контроля и управления доступом**, поскольку около **70%** взломов происходит из-за отсутствия или неправильной работы системы аутентификации.

EFROS DEFENCE OPERATIONS

GIS ГАЗИНФОРМ СЕРВИС

Efros DefOps NAC

– основа для реализации стратегии сетевого доступа с «нулевым доверием»

Многофункциональный комплекс
Efros Defence Operations

EFROS DEFENCE OPERATIONS

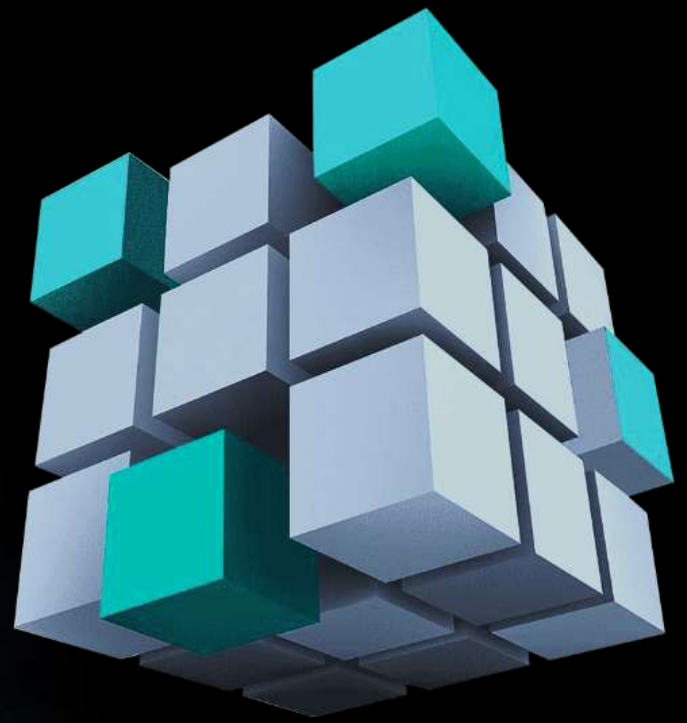
GIS ГАЗИНФОРМ СЕРВИС

NETWORK ACCESS CONTROL
разграничение и контроль доступа в сети

SECURE DNS
защита протокола DNS в корпоративных сетях

FIREWALL ASSURANCE
оптимизация и настройка межсетевых экранов

CHANGE MANAGER
автоматизация процессов управления правилами МЭ



VULNERABILITY CONTROL
анализ уязвимостей и построение векторов атак

NETWORK ASSURANCE
контроль конфигураций АСО и топологии сети, маршрутизация сети

INTEGRITY CHECK COMPLIANCE
контроль целостности и проверки соответствия хостов и конечных точек

Архитектура

EFROS DEFENCE OPERATIONS

GIS ГАЗИНФОРМ СЕРВИС

КОНЕЧНЫЕ ТОЧКИ
(пользователи и устройства)

- ноутбук
- смартфон
- принтер
- видеокамера

СЕТЕВЫЕ УСТРОЙСТВА
(типы подключений)

- Wi-Fi контроллер
- Коммутатор LAN
- VPN-шлюз

Efros DefOps NAC

ВНЕШНИЕ СИСТЕМЫ
(источники и интеграции)

- MS AD / LDAP
- центр сертификатов
- IDM / IGA
- SIEM / SOC
- МСЭ

Факт: атаки через доверенных партнеров стали частым инструментом киберпреступников

EFROS DEFENCE OPERATIONS

GIS ГАЗИНФОРМ СЕРВИС

MITRE | ATT&CK® **T1199: Trusted Relationship**

17% расследований за 2024 год содержало подозрение на компрометацию поставщиков

Актуальность вопросов безопасности рабочих мест

EFROS DEFENCE OPERATIONS

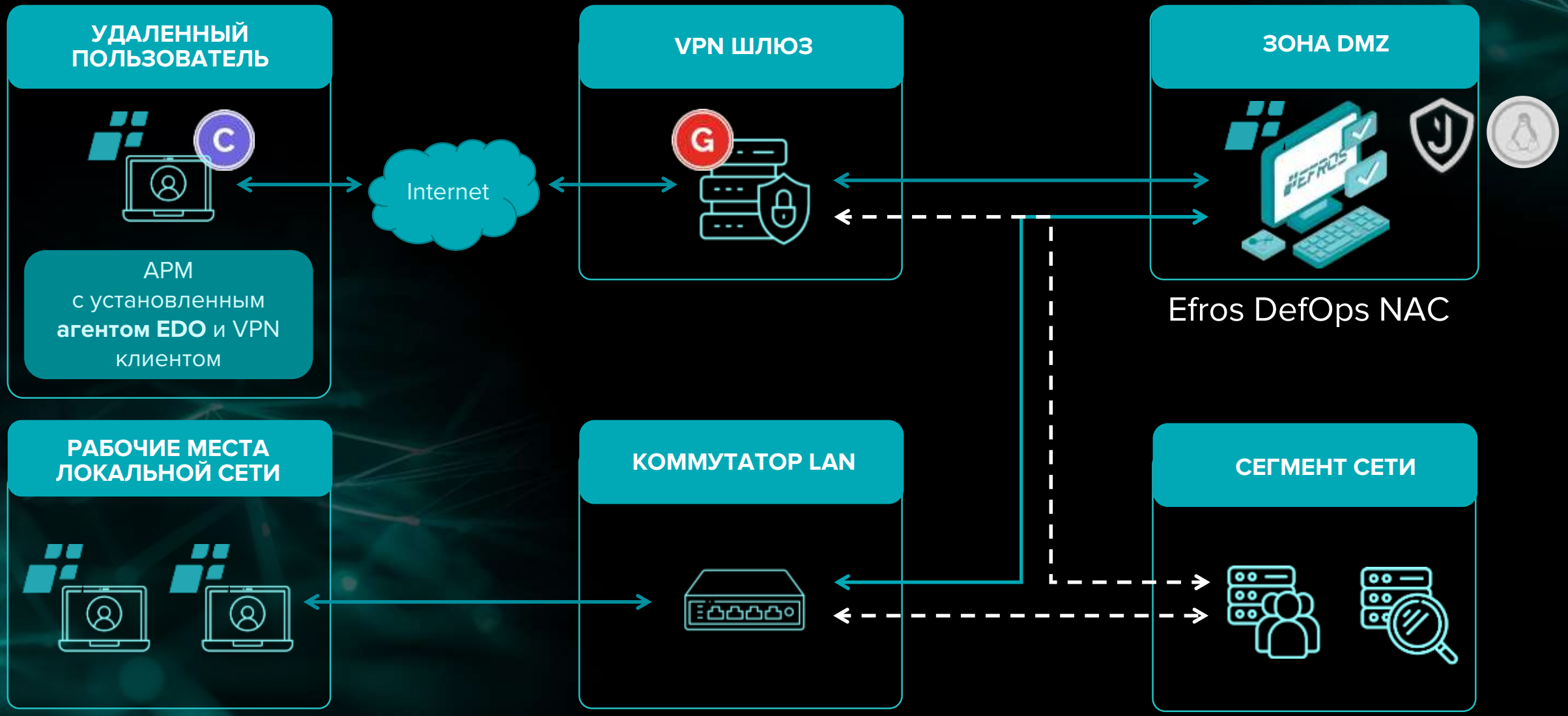
GIS ГАЗИНФОРМ СЕРВИС

1 Безопасность удаленных рабочих мест сотрудников (включая тех, кто подключается со своих устройств – BYOD)

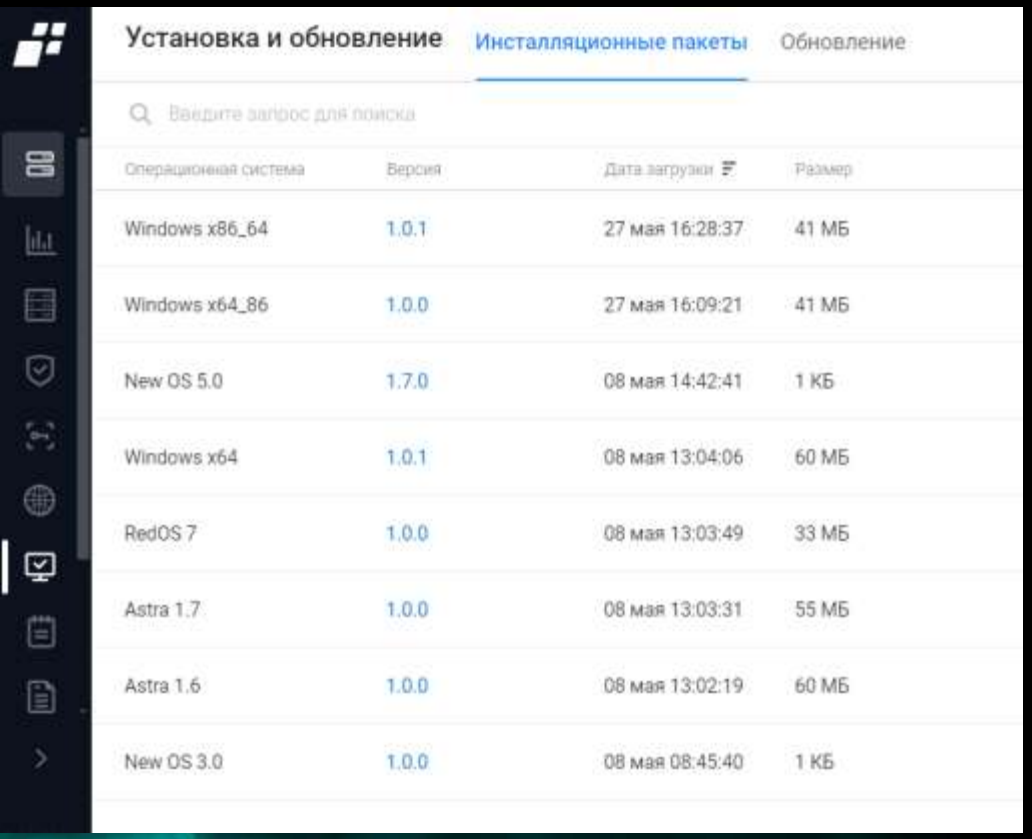
2 Передача на подряд работ, требующих доступ в сеть
Контроль рабочих мест подрядчиков

3 Импортозамещение решений Cisco (AnyConnect выполнял задачи подключения по VPN и оценки – проверки устройств)

Архитектура

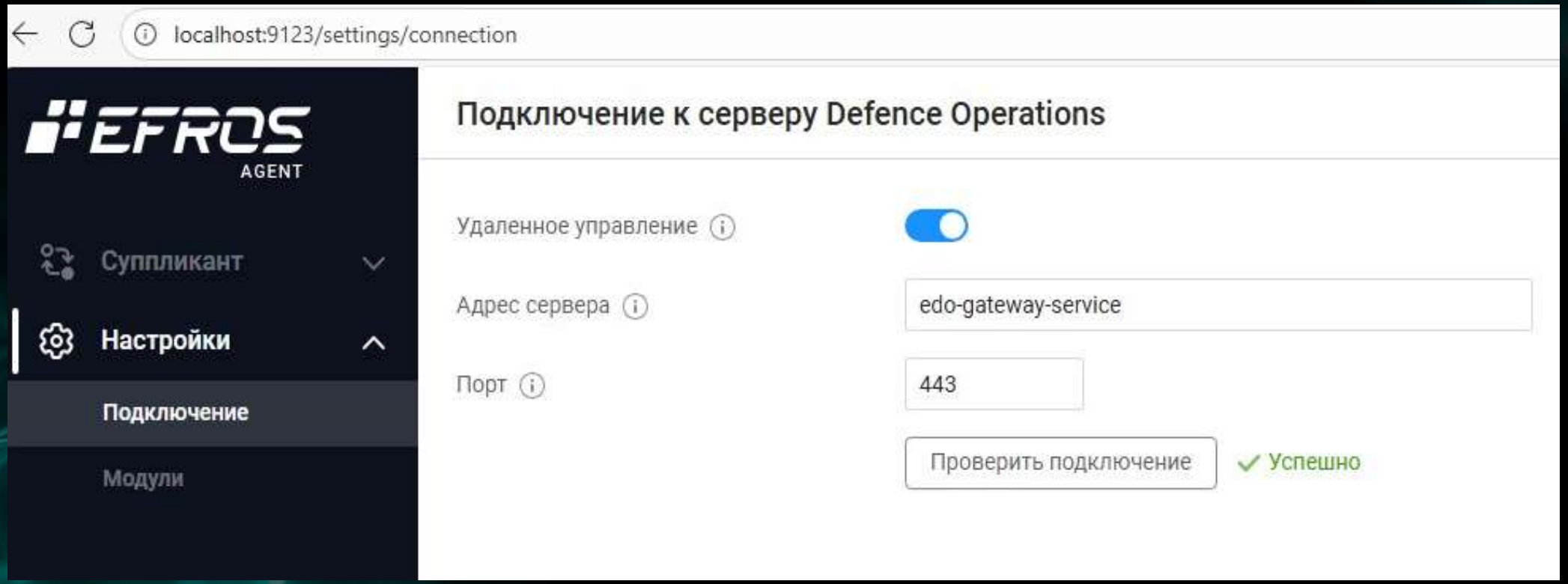


Возможности агента Efros DefOps



- Кроссплатформенное приложение для ОС Windows, Linux, MacOS
- Централизованное обновление через сервер Efros DefOps
- Проверка АРМ на соответствие политикам безопасности по множеству (80+) параметров
- Надежная проверка состояния АВПО от «Лаборатории Касперского»
- Встроенный суппликант для поддержки 802.1x
- Уведомления пользователей при несоответствии политикам (в web-интерфейсе)
- Проверка политики контроля целостности объектов до загрузки ОС
- Сбор логов событий на конечной точке

Агент ПК Efros DO



Агент ПК Efros DO

EFROS DEFENCE OPERATIONS

GIS ГАЗИНФОРМ СЕРВИС

Агенты

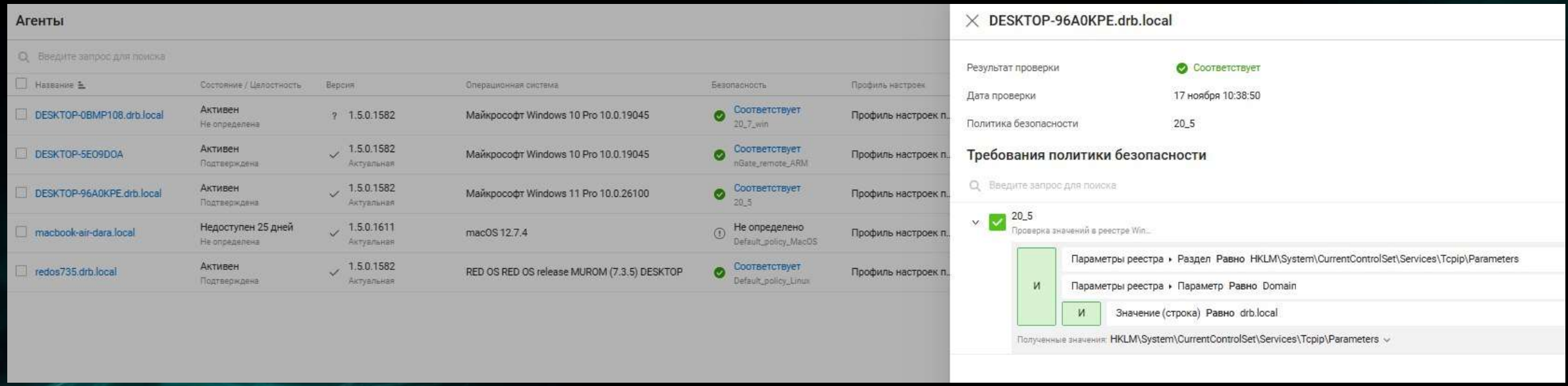
Введите запрос для поиска

Название	Состояние / Целостность	Версия	Операционная система	Безопасность	Профиль настроек	Устройство	Целостность до загрузки ОС
DESKTOP-0BMP108.drb.local	Недоступен только что Не определена	? 1.5.0.1582	Майкрософт Windows 10 Pro 10.0.19045	Не определено 20_7_win	Профиль настроек п...	46 параметров	
DESKTOP-5EO9DOA	Активен Подтверждена	✓ 1.5.0.1582 Актуальная	Майкрософт Windows 10 Pro 10.0.19045	Соответствует nGate_remote_ARM	Профиль настроек п...	27 параметров	
DESKTOP-96A0KPE.drb.local	Активен Подтверждена	? 1.5.0.1582	Майкрософт Windows 11 Pro 10.0.26100	Не соответствует 20_5	Профиль настроек п...	39 параметров	
macbook-air-dara.local	Недоступен 25 дней Не определена	✓ 1.5.0.1611 Актуальная	macOS 12.7.4	Не определено Default_policy_MacOS	Профиль настроек п...	66 параметров	
redos735.drb.local	Активен Подтверждена	✓ 1.5.0.1582 Актуальная	RED OS RED OS release MUROM (7.3.5) DESKTOP	Соответствует Default_policy_Linux	Профиль настроек п...	28 параметров	

Агент ПК Efros DO

EFROS DEFENCE OPERATIONS

GIS ГАЗИНФОРМ СЕРВИС



Агент ПК Efros DO

EFROS DEFENCE OPERATIONS

GIS ГАЗИНФОРМ СЕРВИС

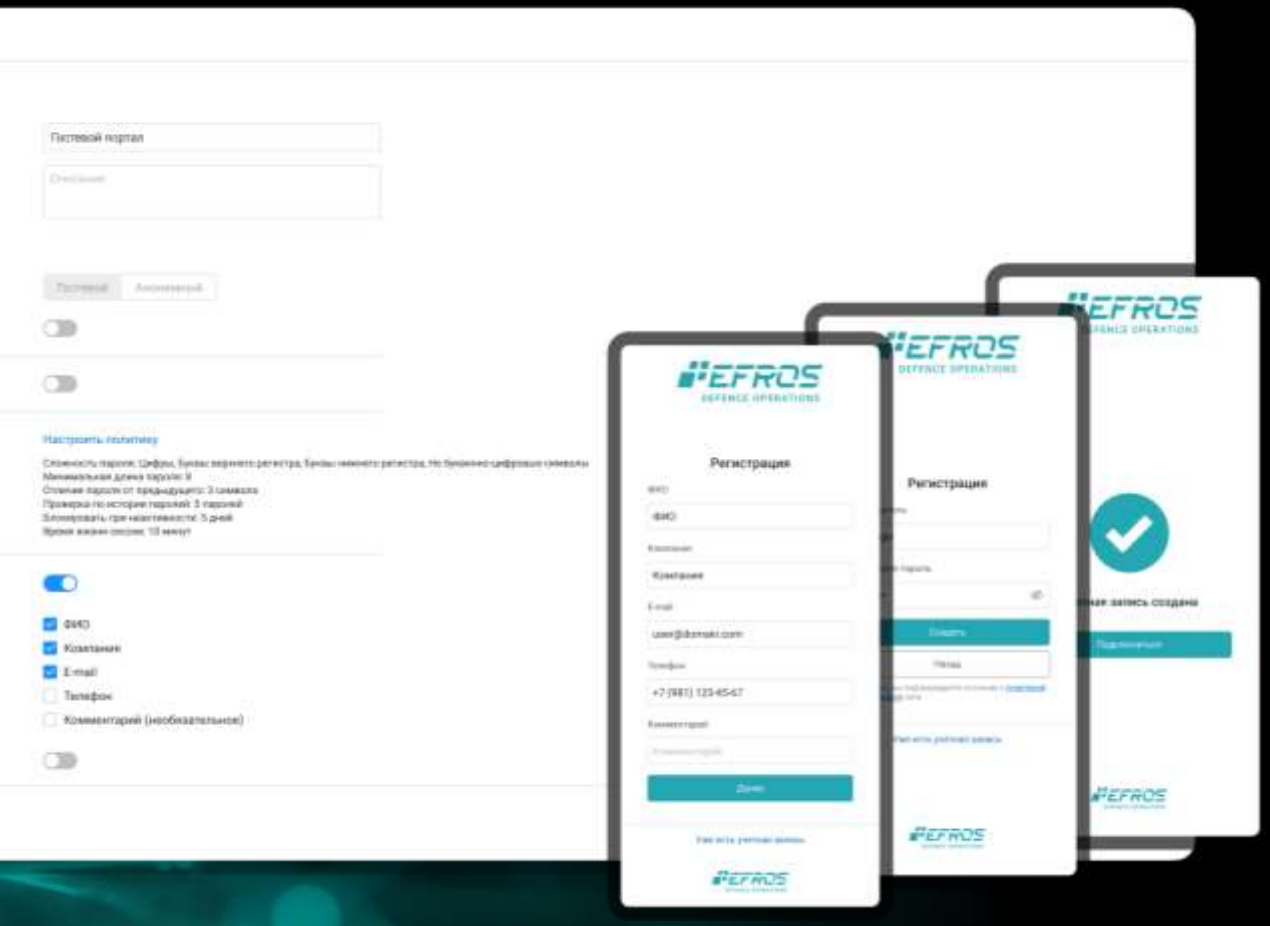
02 ноября 2025 02:46:07

Результат обработки запроса	Доступ предоставлен
IP-адрес устройства	10.10.10.7
Интерфейс устройства	GigabitEthernet1/0/10
Пользователь	artem
Политика доступа	Wired802_1X
Правило аутентификации	EAP-PEAP_MSCHAPv2_REDOS
Правило авторизации	Win11_host_COMPL
Профиль авторизации	COMPLIANT_200

Детализация обработки запроса на доступ

1 Получен Access-Request
4 Определён тип доступа на оборудование: Wired802_1X
8 Найдена политика доступа: "Wired802_1X"
9 Определён набор разрешённых протоколов "Default_Network_Access"
48 Определён тип доступа на оборудование: Wired802_1X
50 Найдено правило аутентификации "EAP-PEAP_MSCHAPv2_REDOS"
52 Найден источник данных домена AD drb
54 Результат аутентификации: ad_DRB-LOCAL: success
62 Найдено правило авторизации "Win11_host_COMPL"
68 Отправка Access-Accept

Контроль доступа и аудит сетевых администраторов



- Ограничение доступа при подключении к сетевому оборудованию (TACACS+)
- Авторизация выполняемых команд на оборудовании
- Журналирование действий администраторов при работе на активном сетевом оборудовании

Импортозамещение

EFROS DEFENCE OPERATIONS

GIS ГАЗИНФОРМ СЕРВИС

Большинство западных компаний-разработчиков ушли с российского рынка, включая **решения NAC для контроля доступа к сети**

Преимущества Efros DefOps NAC и агента Efros DefOps

1 Единое решение для задачи комплаенса и контроля доступа в сеть пользователей и устройств

2 Интеграции с российскими VPN-решениями для контроля безопасности удаленных рабочих мест

3 Соответствие требованиям действующего законодательства в части кибербезопасности и импортозамещения

ROADMAP (агент ПК Efros DO)

EFROS DEFENCE OPERATIONS

GIS ГАЗИНФОРМ СЕРВИС

1 Поддержка уведомлений для клиентов в случае несоответствия политикам

2 Возможность реализации запуска пользовательских скриптов

3 Разработка на клиенте трей-приложения для отображения текущего статуса соответствия и подключения

4 Поддержка РЕДОС 8.0

EFROS
DEFENCE OPERATIONS

GIS ГАЗИНФОРМ СЕРВИС

Остались вопросы?

Андрей Ситников
пресейл-инженер

+7 (812) 677-20-50
sales@gaz-is.ru
EfrosDefOps - website