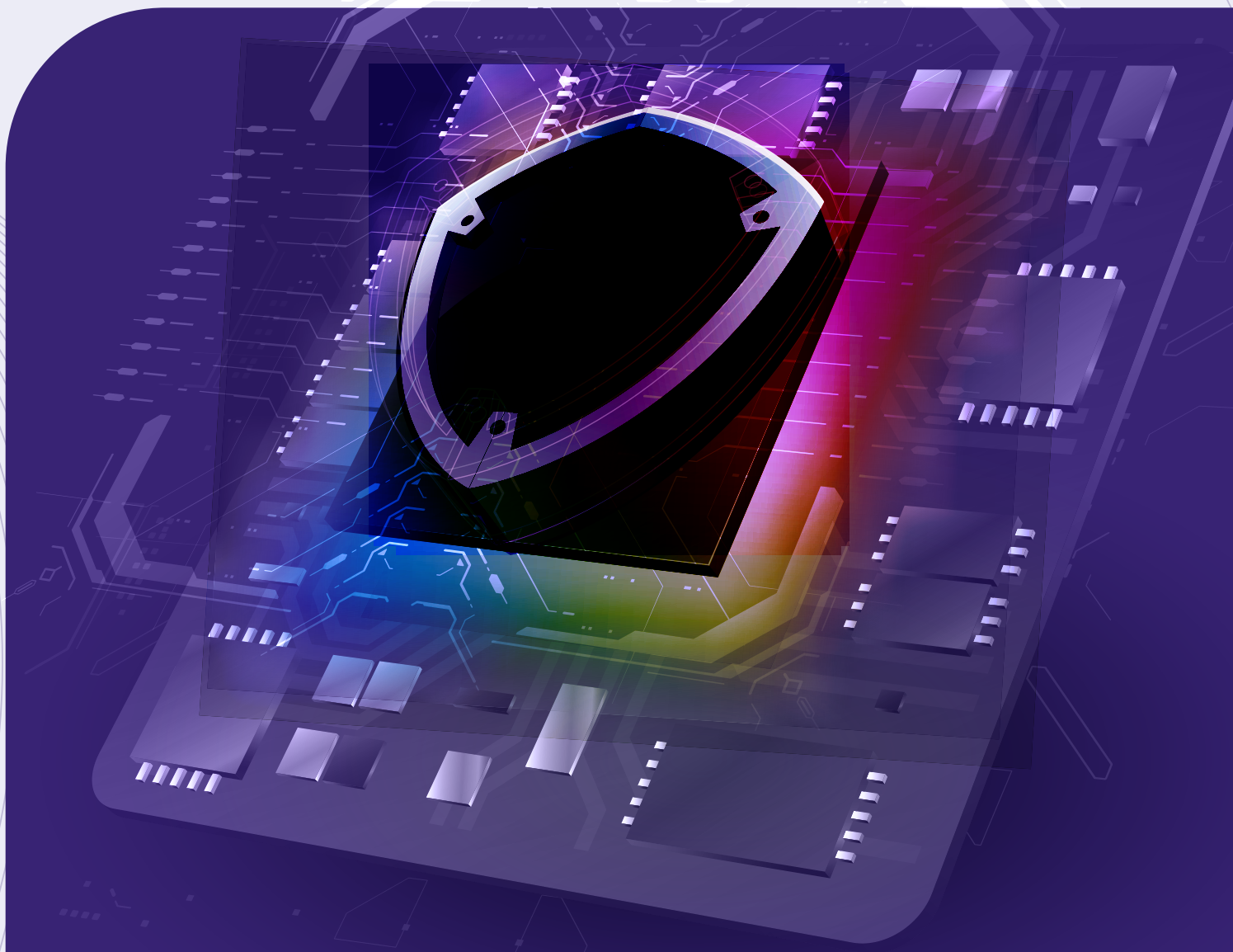
NGRSOFTLAB

NGR Softlab — российский разработчик решений по информационной безопасности



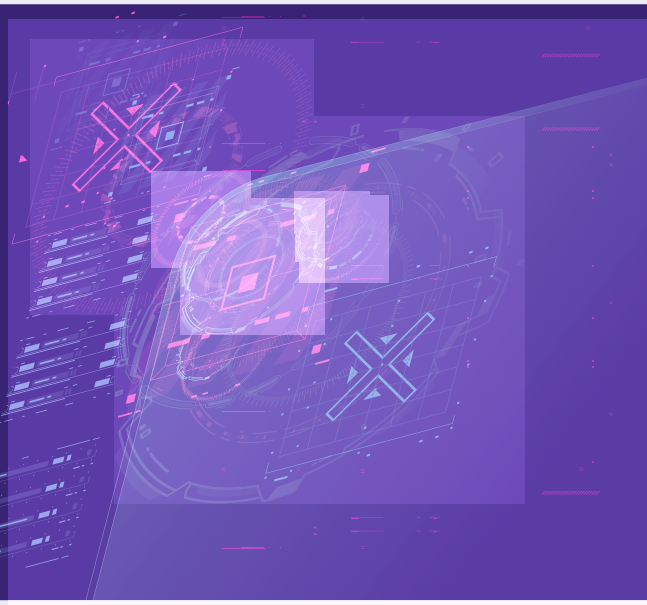
ngrsoftlab.ru

NGRSOFTLAB

Проверенные решения для защиты вашего бизнеса

Компания работает на рынке с 2019 года. В продуктовом портфеле представлены интеллектуальные системы по управлению безопасностью, инструменты анализа и мониторинга ИБ.

Продукты NGR Softlab включены в реестр российского ПО. Центр исследований и производство расположены в России. С 2021 года компания является участником проекта «Сколково» № 1124235.



Рейтинги TADVISER

Топ-85	Топ-90
Крупнейшие поставщики решений в сфере информационной безопасности	Крупнейшие ИТ-поставщики в России

Продуктам NGR Softlab доверяют крупные финансовые организации, компании нефтегазовой отрасли, ритейла и госсектора

Решения разработчика направлены на комплексное повышение безопасности ИТ-инфраструктуры, конкурентоспособности компаний и решение аналитических задач ИБ

Реестр Минцифры РФ

Участник Московский инновационный кластер

КАРТА ИННОВАЦИОННЫХ РЕШЕНИЙ
ID 101245

Участник Sk

Компания предлагает решения, направленные на комплексное повышение безопасности ИТ-инфраструктуры:

ALERTIX
SIEM

SIEM-система для сбора данных, поиска нежелательных событий и обнаружения инцидентов ИБ

DATAPLAN
Security Data Analysis

Аналитическая платформа с использованием алгоритмов машинного обучения для решения задач ИБ

INFRASCOPE
PAM

Комплексный продукт для управления привилегированным доступом класса PAM

ALERTIX
SIEM

NGRSOFTLAB

Платформа Alertix (SIEM)

Платформа Alertix — SIEM-система, предназначенная для сбора и обработки данных от ИБ/ИТ-инфраструктуры организации, поиска нежелательных событий или их комбинаций, обнаружения инцидентов информационной безопасности. Включает инструменты для построения мониторинга ИБ «под ключ».

Alertix позволяет:

- организовать процесс выявления, расследования, учета инцидентов информационной безопасности
- контролировать эффективность ИБ-мониторинга
- экономить на вычислительных ресурсах, отключая неиспользуемые компоненты
- собирать расширенную телеметрию с АРМ и серверов для выявления неизвестных угроз
- повышать эффективность выявления инцидентов с помощью поведенческой аналитики и подключения источников TI
- обеспечить соответствие требованиям ФЗ-187 к объектам КИИ, в том числе взаимодействие с ГосСОПКА

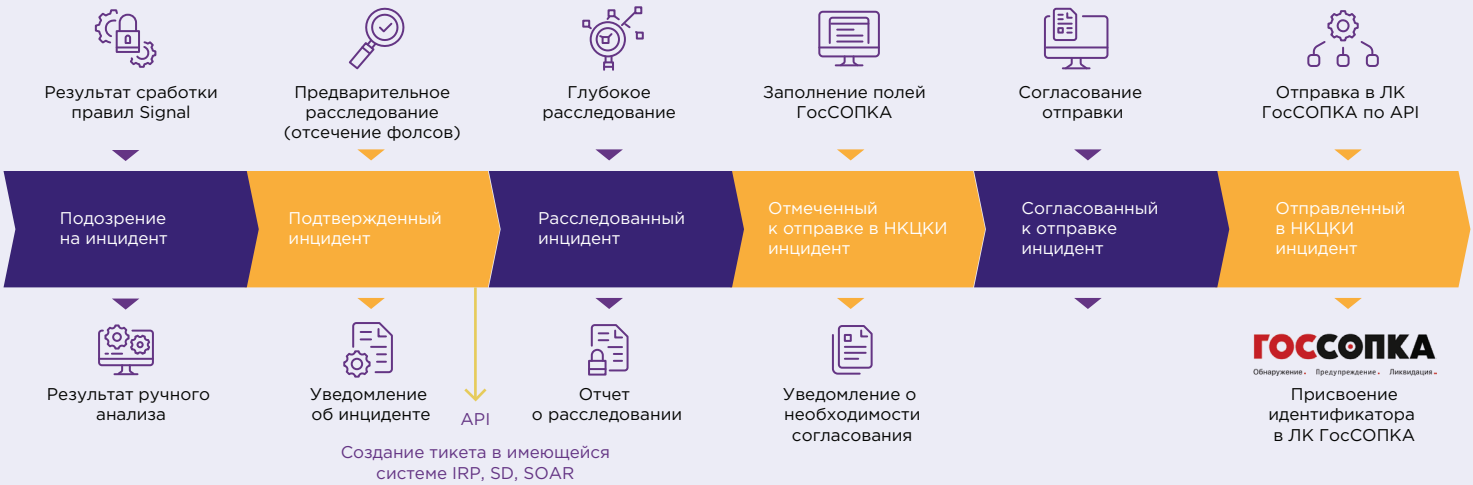
Платформа Alertix обладает высокой гибкостью, позволяя быстро встраиваться в любую ИТ-инфраструктуру, осуществляя сбор и обработку событий.

Сценарии развертывания:

- «все в одном» инсталляции на виртуальном или аппаратном сервере
- распределенная и/или отказоустойчивая инсталляция, включая высоконагруженную
- иерархическая двухуровневая инсталляция с централизацией контроля

Преимущества Alertix:

- полностью российское ПО
- уникальная метрика лицензирования
- встраивается в любую инфраструктуру благодаря высокой гибкости
- непрерывное совершенствование платформы
- отсутствие больших вложений в персонал



Необходимо всего две недели, чтобы внедрить платформу и начать получать пользу

DATAPLAN

NGRSOFTLAB

Dataplan

Dataplan — аналитическая платформа для решения задач ИБ. Анализирует данные с применением алгоритмов машинного обучения для комплексной оценки состояния системы защиты информации, поведения пользователей и элементов инфраструктуры

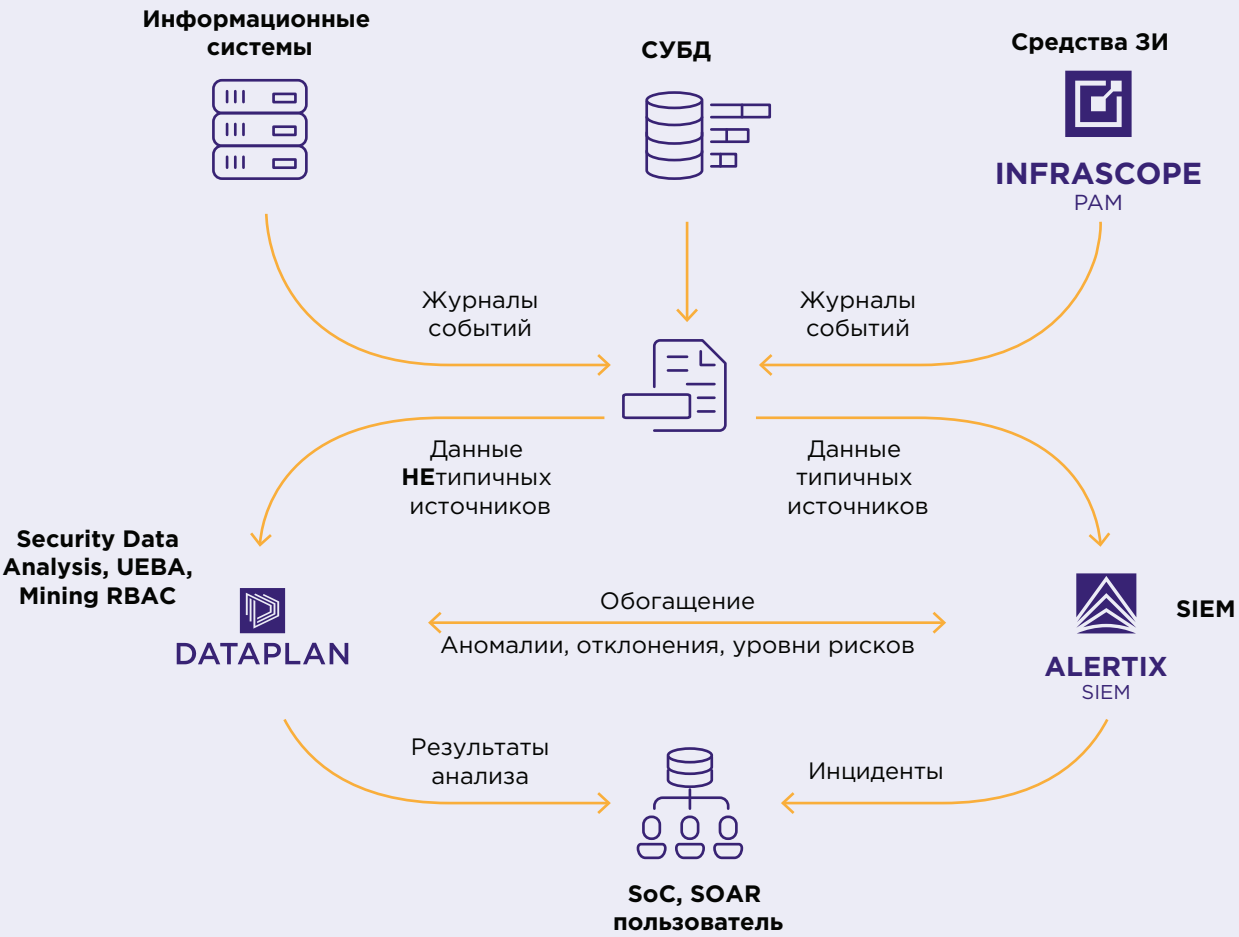
Dataplan предназначен для:

- анализа данных из разных источников и создания индивидуальных систем отчетности (Security Data Analysis)
- расширенной поведенческой аналитики (больше, чем UBA/UEBA)
- формирования ролевой модели и актуализации существующей системы разграничения доступа (Role Mining/RBAC)

Платформа позволяет:

- получить дополнительные сведения для оценки текущего состояния системы защиты информации, инфраструктуры организации
- составить «портрет» пользователя и элементов инфраструктуры
- оптимизировать затраты на внедрение средств защиты от НСД, контроля доступа, предотвращения утечек и пр.
- выявить признаки угроз ИБ, которые не обнаружены типовыми средствами защиты информации

Сценарий применения решения



DATAPLAN

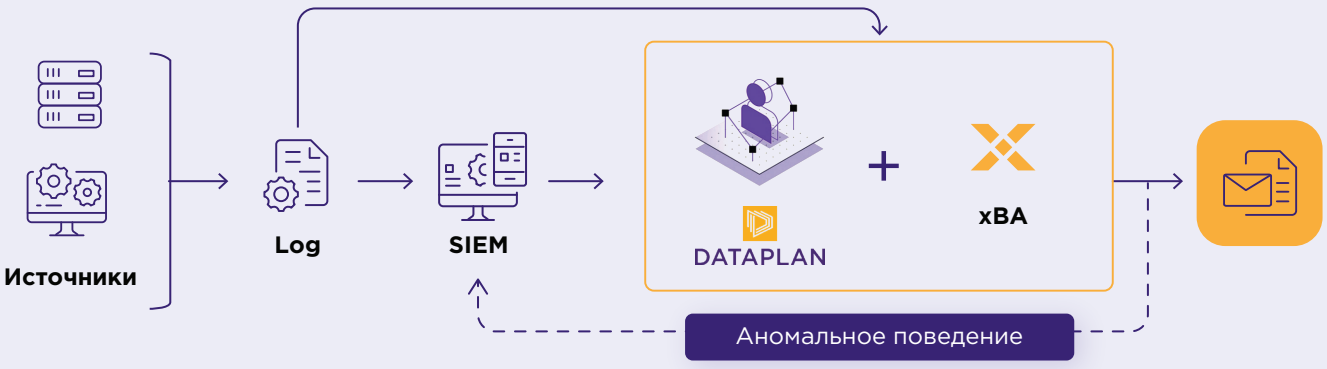
NGRSOFTLAB

Модуль xBA Application

Ежегодно появляются новые, нестандартные действия злоумышленников и вредоносного ПО в ИТ-инфраструктуре, которые способны не только обходить системы защиты, но и скрывать результаты своей деятельности.

Модуль xBA Application
предназначен для поиска и детектирования поведенческих аномалий

- Выполняет круглосуточный мониторинг инфраструктуры, анализирует и хранит данные об активности устройств, ПО, действиях пользователей
- Определяет нормальное поведение сущностей, выявляет аномалии и подозрительную активность, в том числе незамеченную специализированными средствами контроля и защиты, и уведомляет о них
- Выявляет признаки инсайдерской деятельности, компрометации учетных данных, ошибок конфигурации, нарушения политик безопасности, работы вредоносного ПО и нецелевого использования ресурсов



xBA Application – модуль расширения для аналитической платформы Dataplan, выполняет функции класса решений UBA/UEBA

Модуль xBA может взаимодействовать с SIEM-системой

Модуль xBA поможет:

- снизить количество ложных уведомлений об инцидентах
- обогатить сведения о нарушениях дополнительным контекстом
- выполнить анализ характерных действий пользователей или других сущностей, с которыми они взаимодействуют
- выявить индивидуальные или групповые аномалии

DATAPLAN

NGRSOFTLAB

Модуль ролевого моделирования Role Mining Application

Неактуальные права доступа к информационным системам могут предоставить возможность нелегитимного доступа к конфиденциальной информации и спровоцировать существенные риски для бизнеса

Role Mining Application – модуль оценки текущего состояния системы разграничения прав доступа. Предназначен для актуализации правил разграничения доступа, построения и оптимизации ролевой модели.

Модуль Role Mining Application (MVP):

- выполняет анализ Active Directory
- оценивает состояния текущей системы разграничения доступа по ряду метрик и показателей
- определяет группы безопасности и пользователей с наивысшими уровнями риска с помощью встроенных алгоритмов машинного обучения
- формирует рекомендации по оптимизации структуры и системы разграничения доступа

Role Mining Application – модуль расширения для аналитической платформы Dataplan, реализует функции майнинга модели управления доступом на основе ролей (RBAC)

Role Mining Application позволит:

- определить пользователей с лишними правами доступа и группы безопасности с низкой эффективностью
- получить объективную картину доступа к ресурсам, включая ретроспективный анализ
- сократить время предоставления прав для новых сотрудников или при перемещении существующих на новую должность (роль)
- сократить трудоемкость аудита системы разграничения доступа перед внедрением систем управления доступом

INFRASCOPE
PAM

NGRSOFTLAB

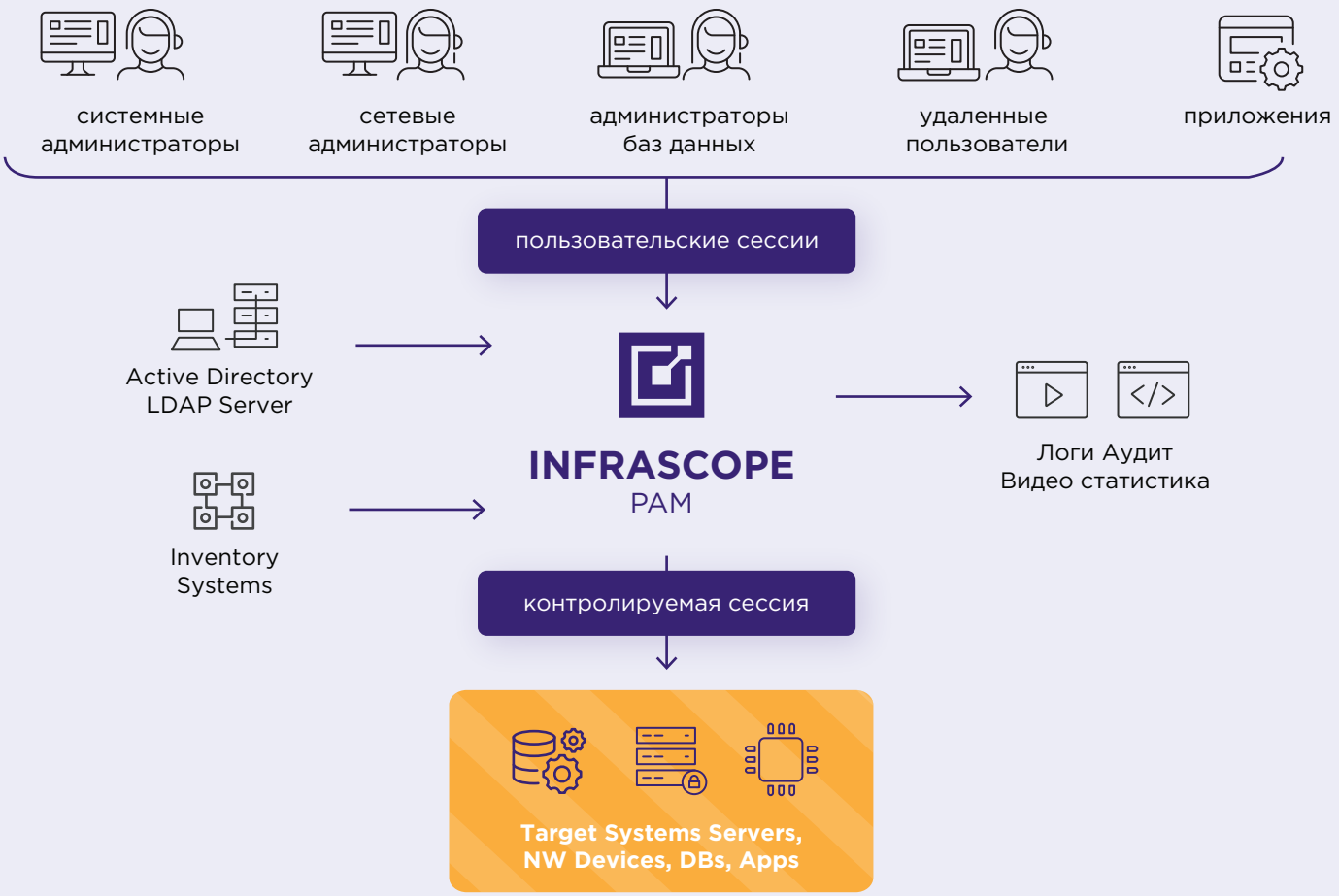
Infrascope

Infrascope — комплексный программный продукт для управления привилегированным доступом класса Privileged Access Management (PAM). Он позволяет защищать доступ к сетевой инфраструктуре и приложениям, а также регистрировать действия, влияющие на непрерывность бизнес-процессов.

Infrascope обнаруживает и предотвращает нарушения, поддерживает возможности индивидуального учета и повышает операционную эффективность за счет управления учетными данными и делегирования привилегированных полномочий.

Решение позволяет:

- отслеживать использование паролей
- облегчать управление доступом для сотен пользователей, подключающихся к тысячам систем
- защищать сторонний удаленный доступ
- управлять с помощью протоколов TACACS+ тысячами сетевых элементов
- ограничить доступ и контролировать действия администраторов баз данных на основе политик черных и белых списков и маскирования при работе с конфиденциальными данными



INFRASCOPE
PAM

NGRSOFTLAB

Infrascope направлен на:

- снижение риска инсайдерских угроз
- защиту от вредоносного ПО и фишинга, нацеленного на привилегированные учетные записи
- обеспечение безопасности аутсорсинговых операций, выполняемых поставщиками и подрядчиками
- проведение аудиторских проверок и формирование отчетности
- снижение уровня привилегий администраторов

Преимущества продукта:

- российское ПО
- безагентское подключение и отсутствие Jump-серверов
- маскирование данных БД при доступе администраторов
- оперативное развертывание
- модульность
- масштабируемость
- предотвращение действий в реальном времени

Менеджер паролей

Безопасное и эффективное управление паролями устройств и баз данных

TACACS+ менеджер доступа

Объединение AAA, Active Directory, LDAP и TACACS+

2FA-менеджер

Аутентификация с помощью комбинации двух различных компонентов

Менеджер сессий

Логирование и запись всех сеансов, включая командную и контекстную фильтрацию

Менеджер доступа к данным

Журналирование доступа с возможностью применения политик и маскирования в режиме реального времени

NGRSOFTLAB

NGR SOFTLAB

121087, Москва, ул. Барклая д.6, стр.5, БЦ «Барклай Плаза», офис 306

+7 (495) 269-29-59 | info@ngrsoftlab.ru

vk.com/ngrsoftlab

ngrsoftlab.ru