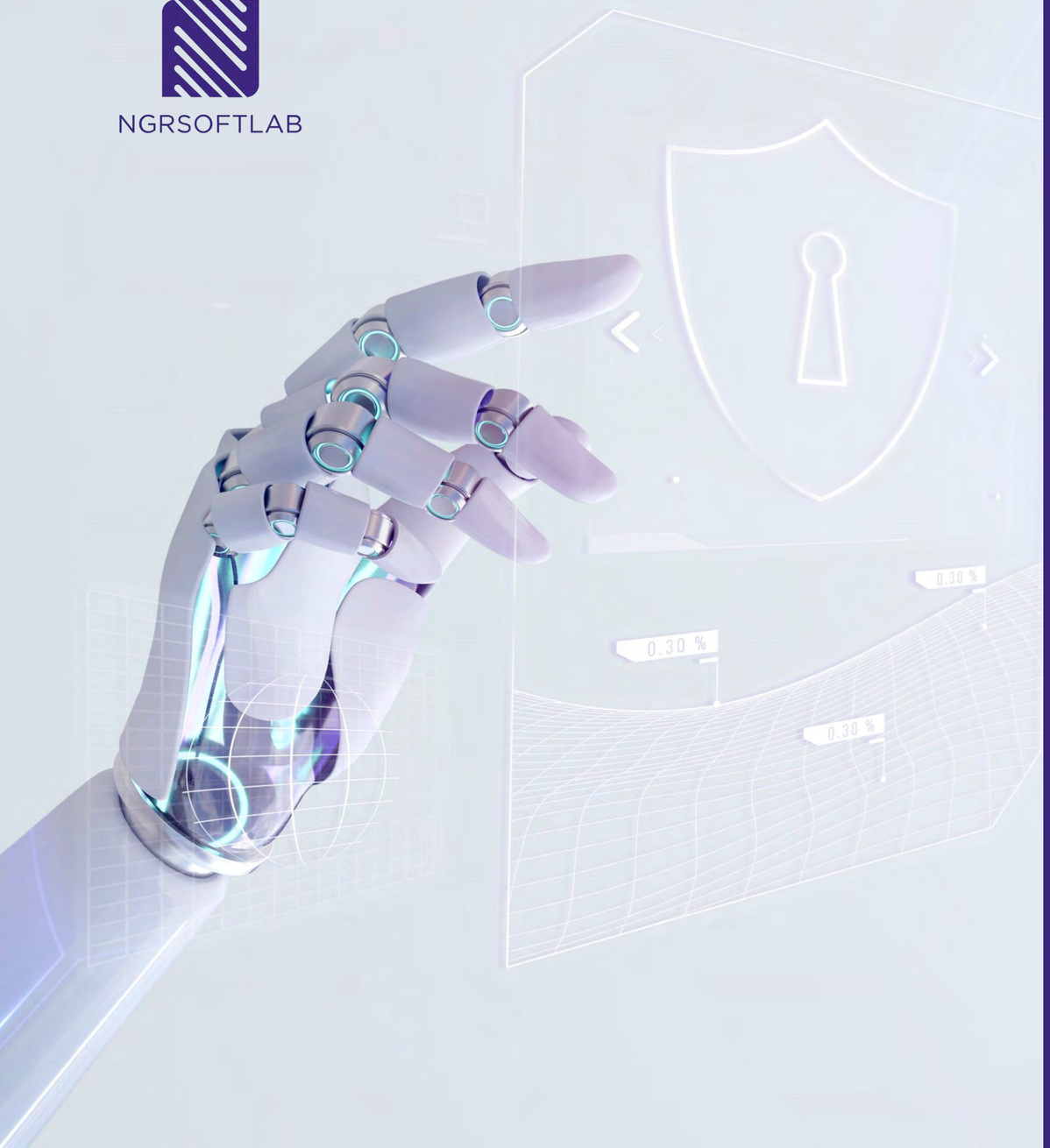
NGRSOFTLAB

INFRASCOPE
PRIVILEGED ACCESS MANAGEMENT

Управление и защита
привилегированным
доступом

NGRSOFTLAB



NGR Softlab — прогрессивная команда ИТ-специалистов

в области разработки средств ИБ, обработки и анализа данных, а также роботизации бизнес-процессов

01 Работаем на территории РФ, учитываем требования и условия отечественного рынка

02 Нацелены на создание полезных и технологичных решений

03 Накапливаем экспертизу, делимся опытом в наших продуктах

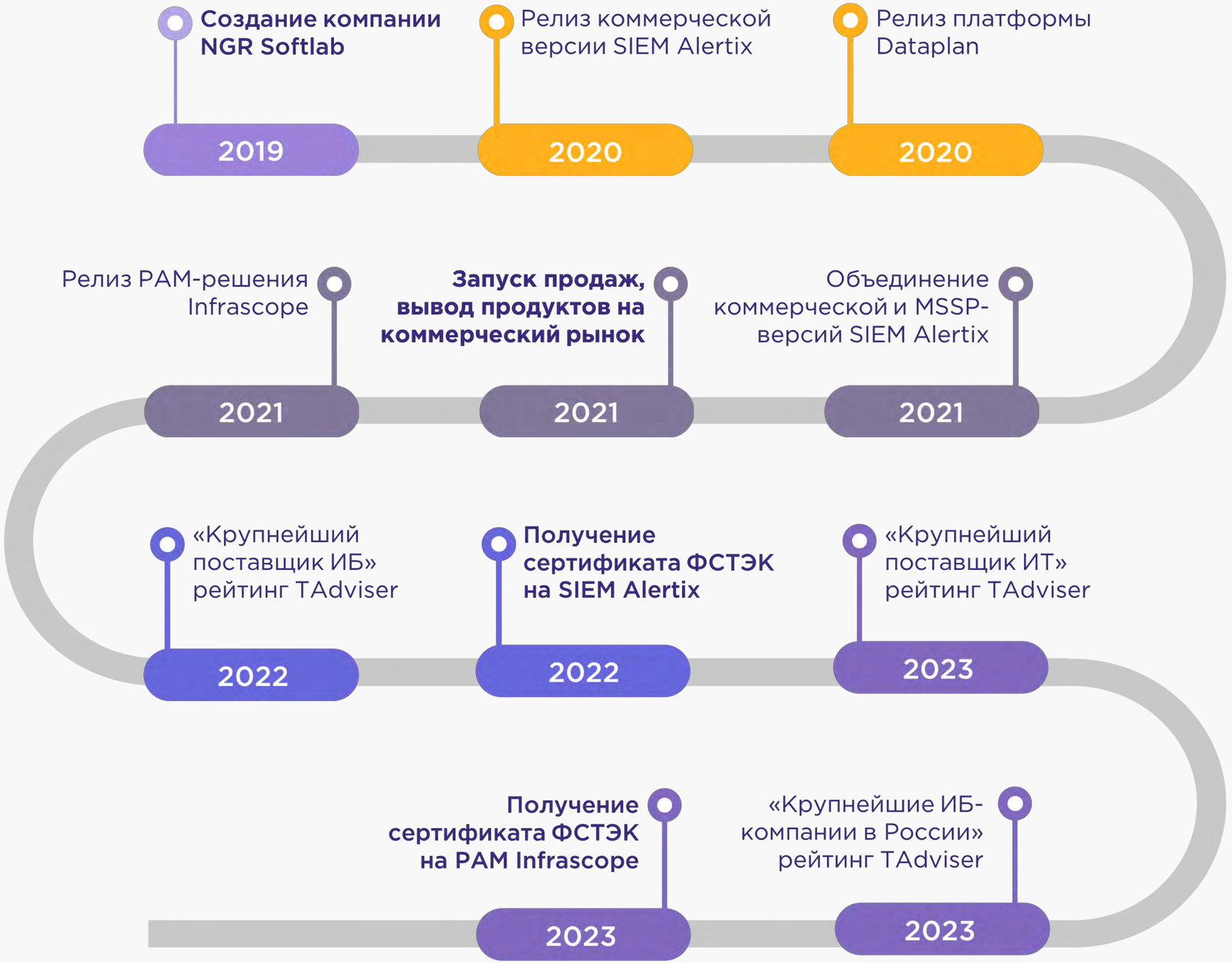
04 Участник инновационного кластера Москвы

05 Лицензии ФСТЭК России № 1939 от 30.03.2020 (СЗКИ), № 3743 от 30.03.2020 (ТЗКИ)

06 СМК соответствует требованиям ГОСТ Р ИСО 9001-2015

NGRSOFTLAB

ИСТОРИЯ РАЗВИТИЯ КОМПАНИИ



СИНЕРГИЯ ПРОДУКТОВ NGR SOFTLAB

NGRSOFTLAB

DATAPLAN

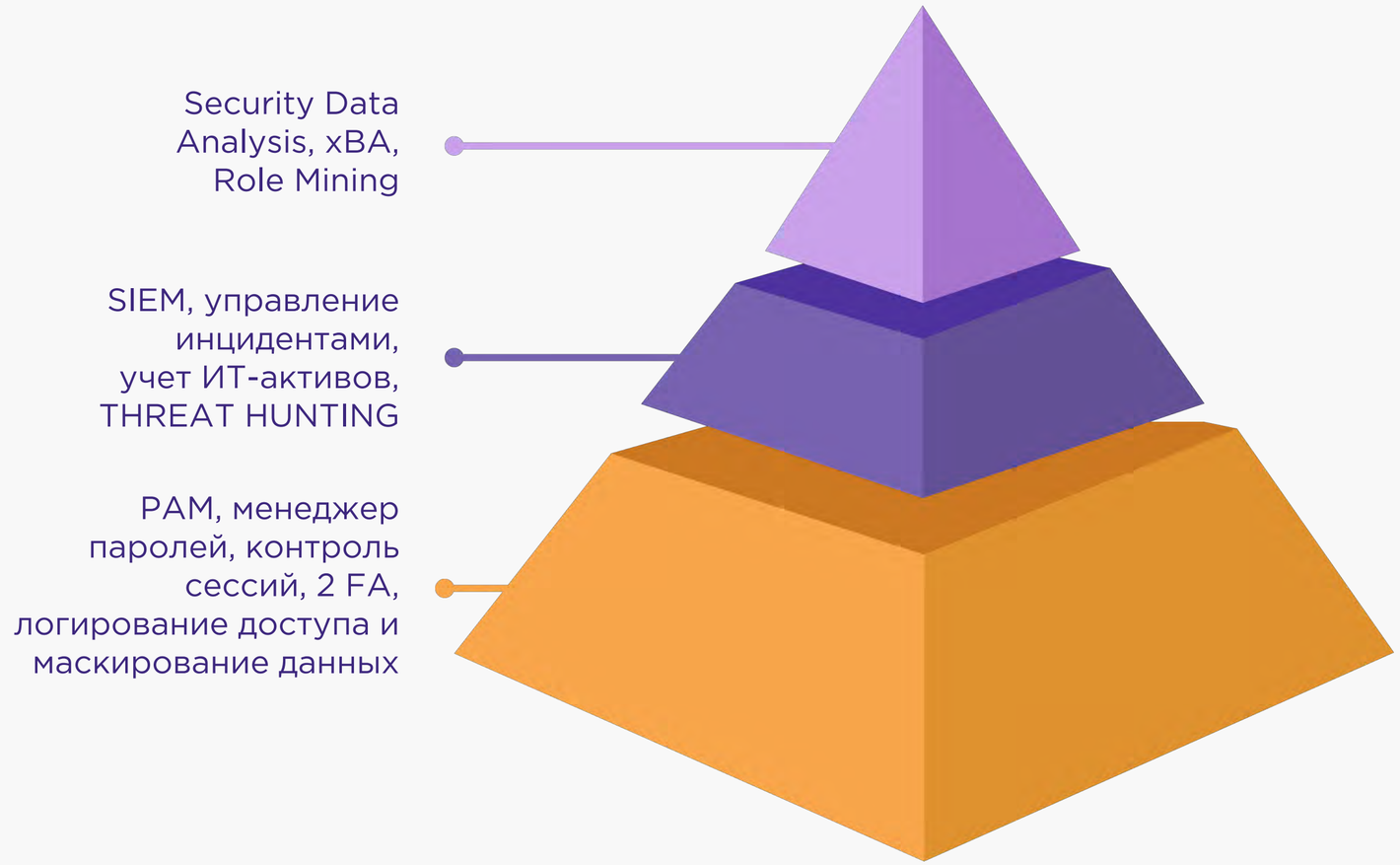
Аналитическая платформа для решения задач ИБ. Анализирует данные с применением алгоритмов машинного обучения для комплексной оценки системы защиты информации, поведения пользователей и элементов инфраструктуры. Включает модули UEBA и оптимизации RBAC

ALERTIX

SIEM-система и набор дополнительных инструментов, разработанные с учетом лучших практик коммерческого SOC-центра. Имеет сертификат ФСТЭК №4596. Подтверждает соответствие требованиям безопасности информации по четвертому уровню доверия

INFRASCOPE

PAM-решение, предназначенное для управления и защиты привилегированного доступа, мониторинга и протоколирования действий пользователей с расширенным набором прав. Имеет сертификат ФСТЭК №4752. Выполняет уникальные для данного класса решений функции



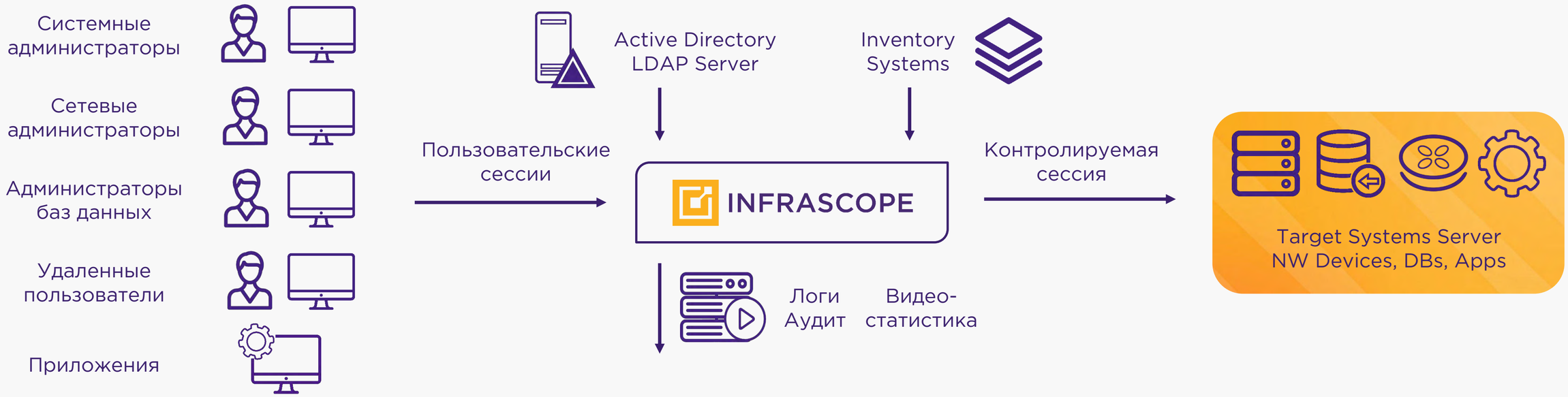
NGRSOFTLAB

INFRASCOPE

NGRSOFTLAB

INFRASCOPE: СХЕМА РАБОТЫ

Комплексный продукт для управления привилегированным доступом (PAM), разработанный для предотвращения внутренних и внешних атак с целью взлома привилегированных учетных записей. Позволяет защищать доступ к сетевой инфраструктуре и приложениям, а также регистрировать действия, влияющие на непрерывность бизнес-процессов.



Соответствует ГОСТ 57580 «Безопасность финансовых (банковских) операций»

NGRSOFTLAB

INFRASCOPE: АРХИТЕКТУРА РЕШЕНИЯ

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Поставляется как образ VM для VMware

Работает на Linux

Хранилище данных в PostgreSQL

ВЫСОКАЯ ДОСТУПНОСТЬ

Минимальная лицензия — 2 системные единицы

Резервное копирование

Репликация и синхронизация

Подход «active-active»

NGRSOFTLAB

INFRASCOPE: РАСШИРЕННЫЕ ВОЗМОЖНОСТИ

КОНТРОЛЕР

Для крупных распределенных систем

Контроль инцидентов

Централизованное хранилище данных

Репликация и синхронизация

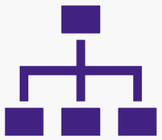
Централизованный быстрый поиск

ИЗОЛИРОВАННАЯ СРЕДА ИСПОЛНЕНИЯ

Изолированный контур

Управление привилегированными сессиями

Секретное хранилище



Распределение пользователей и устройств

NGRSOFTLAB

INFRASCOPE: МОДУЛИ ПРОДУКТА

Менеджер паролей

Управляет паролями устройств и баз данных, обеспечивая безопасность с сохранением эффективности

Менеджер сессий

Логирование и запись всех сеансов, включая командную и контекстную фильтрацию

2FA менеджер

Дополнительный уровень аутентификации пользователей с помощью комбинации двух различных компонентов

TACACS+ Менеджер доступа

Программное обеспечение безопасности на основе протокола объединяет AAA, Active Directory, LDAP и TACACS+

Менеджер доступа к данным

Журналирование доступа к данным с возможностью применения политик и маскирования данных в реальном времени

AAPM менеджер

Управляет учетными записями приложений обеспечивая их выдачу через API

NGRSOFTLAB

МЕНЕДЖЕР ПАРОЛЕЙ

NGRSOFTLAB

INFRASCOPE, МЕНЕДЖЕР ПАРОЛЕЙ: О МОДУЛЕ

Протоколы

- SSH / Telnet-протокол
- Active Directory LDAP / LDAPS
- SMB / RDP / VNC
- HTTPS / HTTP
- Базы данных*
- Клиентский протокол

Размерность

Пользователи

БЕЗ ЛИМИТА

Сохраненные аккаунты

БЕЗ ЛИМИТА

Функциональность

- Секретное хранилище
- Мультиаккаунт-подключение к разным устройствам с 1 УЗ
- Автоматическая смена паролей
- Политики усиления паролей
- Статические ключи
- Управление SSH-ключами
- Обнаружение привилегированных аккаунтов
- Доступ через разрешения
- Полное логирование с быстрым поиском
- Пароли для Apps (AAPM)
- API для интеграций

**Поддерживаемые базы данных: Oracle, MS SQL, PostgreSQL, MySQL, Teradata, SAP HANA, Cassandra и др.*

NGRSOFTLAB

INFRASCOPE, МЕНЕДЖЕР ПАРОЛЕЙ: ЭФФЕКТ ОТ ИСПОЛЬЗОВАНИЯ

ПРОБЛЕМАТИКА

Простые пароли

Отслеживание паролей
(кто использовал, когда и почему)

Использование одного и того же пароля для многих систем

Данные УЗ хранятся в БД, исходных кодах или конфигурационных файлах,

Обмен паролями среди коллег

Пароли не изменяются
через равные промежутки времени

РЕШЕНИЕ

- ✓ Предотвращение несанкционированного доступа к критическим системам
- ✓ Прекращение атак с использованием украденных привилегированных учетных данных
- ✓ Обеспечение контроля доступа на основе ролей
- ✓ Изменение паролей регулярно и после каждого использования
- ✓ Исключение совместного использования паролей среди сотрудников
- ✓ Автоматическая блокировка учетной записи пользователя при увольнении сотрудника
- ✓ Исключение встроенных паролей, которые хранятся в незашифрованных текстовых файлах, БД или исходных кодах

NGRSOFTLAB

МЕНЕДЖЕР СЕССИЙ

NGRSOFTLAB

INFRASCOPE, МЕНЕДЖЕР СЕССИЙ: О МОДУЛЕ

Протоколы

- SSH / Telnet-протокол
- RDP / VNC
- HTTPS / HTTP
- SFTP

Размерность

Функциональность

- SSO
- Настраиваемые политики
- Мониторинг и прекращение активных сессий
- Запись видео и входных данных с помощью OCR
- Процедуры разрешений соединений и команд
- Настраиваемая ролевая модель
- Ревизия данных и SIEM-интеграция
- Полное логирование с быстрым поиском

Поддерживаемые устройства

- ✓ **MS Windows** (любая версия)
- ✓ **Linux / Unix** (Debian, Ubuntu, Red Hat, CentOS, MacOS и др.)
- ✓ **Сетевое оборудование** любого вендора (роутеры, коммутаторы и др.)
- ✓ **Hardware / software** с заявленными требованиями

NGRSOFTLAB

INFRASCOPE, МЕНЕДЖЕР СЕССИЙ: ЭФФЕКТ ОТ ИСПОЛЬЗОВАНИЯ

ПРОБЛЕМАТИКА

Сложность управления доступом (сотни пользователей подключаются к тысячам систем)

Отсутствие центральной точки контроля доступа для критически важных систем

Предоставление пользователям больших привилегий, чем нужно

Боковое продвижение злоумышленника и распространение вредоносного ПО в критические системы

Незащищенный сторонний удаленный доступ

Отсутствие данных и отчетов для аудита и соответствия нормативным требованиям

РЕШЕНИЕ

- ✓ Просмотр сессий с возможностью поиска в журналах команд и нажатия клавиш
- ✓ Выделение критических целевых систем из пользовательской сети
- ✓ Предоставление функции с наименьшими привилегиями, включая ограничения на основе команд или приложений, утверждение администратором и т.д.
- ✓ Обнаруживает и останавливает вредоносные действия до их возникновения
- ✓ Пользователи продолжают беспрепятственно использовать свои собственные клиентские приложения
- ✓ Обеспечивает централизованную политику безопасности на основе ролей

NGRSOFTLAB

2FA МЕНЕДЖЕР

NGRSOFTLAB

INFRASCOPE, 2FA-МЕНЕДЖЕР: О МОДУЛЕ

Каналы

Email

Mobile

Функциональность

Фактор:
online OTP

2FA для сторонних
решений

Настраиваемая
интеграция

Совместимость

Яндекс Ключ

Google
Authenticator

Microsoft
Authenticator

NGRSOFTLAB

INFRASCOPE, 2FA-МЕНЕДЖЕР: ЭФФЕКТ ОТ ИСПОЛЬЗОВАНИЯ

ПРОБЛЕМАТИКА

- Защита внешних подключений приложений
- Кража аккаунтов с помощью фишинга, вредоносных программ и т.д.
- Легко обнаружить учетные данные пользователя
- Необходимы дополнительные меры предосторожности для доступа третьих лиц и удаленных подключений

РЕШЕНИЕ

- ✓ Предотвращает несанкционированный доступ, даже если учетная запись пользователя украдена
- ✓ Усиливает процесс входа в систему, даже если пароль слабый или неизменный, предоставляя одноразовые токены
- ✓ Устраняет риски обмена паролями среди коллег
- ✓ Включает двухфакторную авторизацию для внешних приложений

NGRSOFTLAB

TACACS+ МЕНЕДЖЕР

NGRSOFTLAB

INFRASCOPE, TACACS+ МЕНЕДЖЕР: О МОДУЛЕ

Протоколы

TACACS+

Размерность

Функциональность

- AAA-система
- SSO
- Авторизация по настраиваемым политикам
- Для любого оборудования
- Долгосрочное хранение логов
- Поддержка сети любого объема
- Замена любой AAA-системы
- Полное логирование с быстрым поиском

Поддерживаемые устройства

UserGate, ZTE, HUAWEI, infotecs, JUNIPER NETWORKS, CISCO, ELTEX SOLUTIONS, НАТЕКС, McAfee, QTECH МИР ДОСТУПНЕЕ, FORTINET, citrix

NGRSOFTLAB

INFRASCOPE, TACACS+ МЕНЕДЖЕР: ЭФФЕКТ ОТ ИСПОЛЬЗОВАНИЯ

ПРОБЛЕМАТИКА

Устаревшие сетевые элементы, которыми нужно управлять

Сложность устаревших моделей определения политики TACACS+

Несколько серверов TACACS+ для разных отделов в пределах одного предприятия

Состояние окончания срока службы Cisco ACS

РЕШЕНИЕ

- ✓ Автономное серверное решение AAA для протокола TACACS+
- ✓ Предоставляет функции с наименьшими привилегиями, включая ограничения на основе команд и уровня привилегий
- ✓ Применяет политики безопасности централизованно для прямого подключения к сетевым элементам
- ✓ Поддерживает настройку пользовательских определений AVP (пары «атрибут-значение»)
- ✓ Высокая производительность и масштабируемость

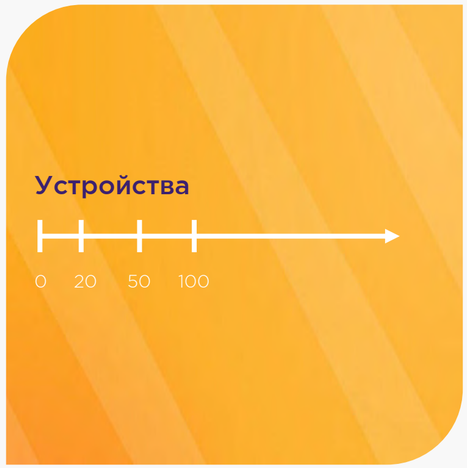
NGRSOFTLAB

МЕНЕДЖЕР ДОСТУПА К ДАННЫМ

NGRSOFTLAB

INFRASCOPE, МЕНЕДЖЕР ДОСТУПА К ДАННЫМ: О МОДУЛЕ

Размерность



Функциональность

- SSO
- Политики SQL-запросов
- Авторизация по настраиваемым политикам
- Запись запросов
- Долгосрочное хранение логов
- Соответствие законодательству
- Маскирование данных
- Полное логирование с быстрым поиском

Поддерживаемые базы данных

Couchbase, MySQL, cassandra, ORACLE DATABASE, Microsoft SQL Server, IBM DB2, teradata., PostgreSQL, HIVE, SAP HANA

NGRSOFTLAB

INFRASCOPE, МЕНЕДЖЕР ДОСТУПА К ДАННЫМ: ЭФФЕКТ ОТ ИСПОЛЬЗОВАНИЯ

ПРОБЛЕМАТИКА

Администраторы БД с высоким уровнем привилегий могут просматривать, изменять любые конфиденциальные данные

Отсутствие централизованного контроля доступа к источникам данных

Компромисс между уровнем безопасности и производительностью баз данных

Незащищенный сторонний удаленный доступ к источникам данных

РЕШЕНИЕ

- ✓ Логирование всех запросов
- ✓ Централизованное обеспечение основанной на ролях политики безопасности доступа к данным
- ✓ Отсутствие снижения производительности на целевых базах данных
- ✓ Пользователи продолжают беспрепятственно использовать свои собственные клиентские приложения
- ✓ Обнаружение конфиденциальных данных в источниках данных
- ✓ Маскирование данных на лету без изменения исходных данных
- ✓ Поддерживает широкий спектр баз данных и защищенных серверов передачи файлов

NGRSOFTLAB

AAPM
МЕНЕДЖЕР

NGRSOFTLAB

INFRASCOPE, AAPM-МЕНЕДЖЕР: О МОДУЛЕ

Размерность

Пользователи

БЕЗ ЛИМИТА

Сохраненные аккаунты

БЕЗ ЛИМИТА

API-запросы

БЕЗ ЛИМИТА

Функциональность

- Секретное хранилище
- Авторизация по настраиваемым политикам
- Автоматическая смена паролей
- Политики усиления паролей
- Управление SSH-ключами
- API для интеграций
- Поддержка сети любого объема
- Полное логирование с быстрым поиском
- Статические ключи
- Высокая доступность

NGRSOFTLAB

INFRASCOPE, AAPM-МЕНЕДЖЕР: ЭФФЕКТ ОТ ИСПОЛЬЗОВАНИЯ

ПРОБЛЕМАТИКА

Пароли в скриптах хранятся в открытом виде

Отсутствует логирование и контроль обращений к целевой системе

При изменении пароля на целевой системе необходимо вносить изменения в скрипты

Пароли могут не соответствовать парольной политике

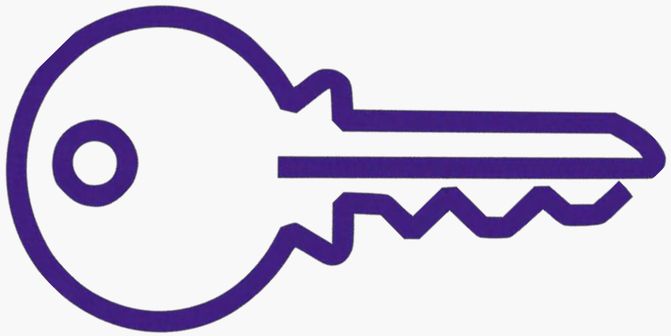
Отсутствует возможность быстрой смены паролей

РЕШЕНИЕ

- ✓ API-запросы на предоставление пароля с использованием token и дополнительных методов аутентификации
- ✓ Привязка token к пользователю/группам пользователей
- ✓ Контроль срока жизни token (дата истечения, количество обращений)
- ✓ Привязка нескольких аккаунтов к одному token
- ✓ Логирование запросов к AAPM
- ✓ Централизованное хранение паролей от целевых систем
- ✓ Централизованное применение парольных политик
- ✓ Централизованная смена паролей

NGRSOFTLAB

INFRASCOPE: КЛЮЧЕВЫЕ ПРЕИМУЩЕСТВА



- Безагентское подключение
- Централизация
- Модульность, масштабируемость
- Прозрачность
- Маскирование данных в БД
- Сертификат соответствия на все модули
- Скорость развертывания
- Предотвращение в реальном времени
- Нет jump-серверов

NGRSOFTLAB

NGR SOFTLAB

Телефон **+7 (495) 269-29-59**

Почта **info@ngrsoftlab.ru**

Сайт **ngrsoftlab.ru**

127018, Москва, БЦ «Двинцев»,
ул. Двинцев, 12к1С