NGRSOFTLAB

INFRASCOPE

Безопасность и эффективность управления
сетевыми ресурсами

О компании

NGR Softlab — российский разработчик средств обработки и анализа данных, роботизации бизнес-процессов и решений в области информационной безопасности.

- Нацелена на создание современных и технологичных продуктов.
- R&D и производство расположены в России и ориентированы на российского потребителя.

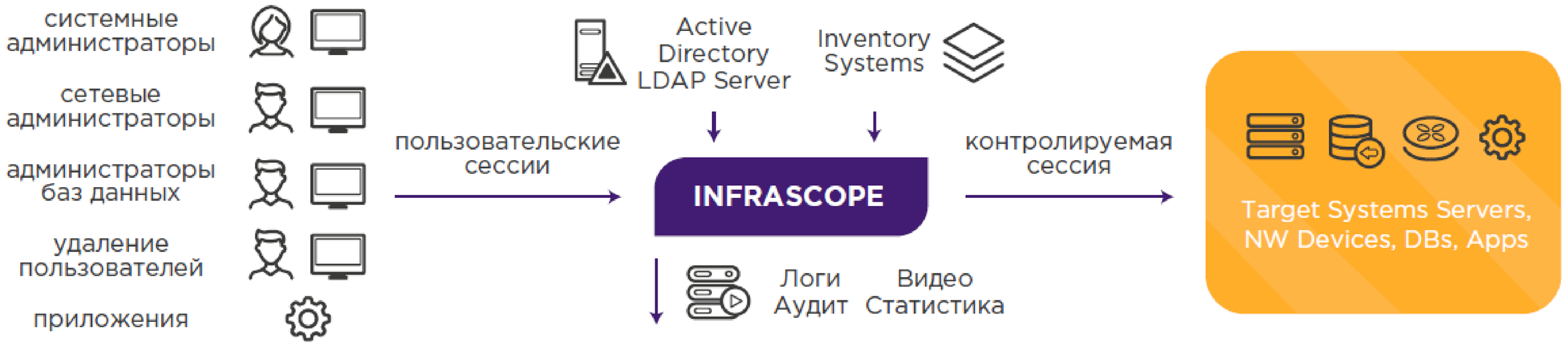
ЭКОСИСТЕМА ПРОДУКТОВ NGR SOFTLAB
Синергия и расширение функционала

INFRASCOPE
USER ACTIONS VISIBILITY

Infrascope — комплексный продукт для управления привилегированным доступом (PAM), разработанный для предотвращения внутренних и внешних атак с целью взлома привилегированных учетных записей.

Полный набор инструментов и функций, которые помогают обеспечивать контроль, управление и осуществлять мониторинг привилегированных пользователей в режиме реального времени с возможностью записи всех действий.

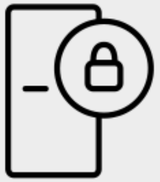
INFRASCOPE


системные администраторы
сетевые администраторы
администраторы баз данных
удаление пользователей
приложения
Active Directory LDAP Server
Inventory Systems
пользовательские сессии
INFRASCOPE
контролируемая сессия
Target Systems Servers, NW Devices, DBs, Apps
Логи
Аудит
Видео
Статистика

МОДУЛИ INFRASCOPE

Менеджер паролей

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



TACACS+ Менеджер доступа

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

Менеджер сессий

Логирование и запись всех сеансов, включая командную и контекстную фильтрацию

Менеджер доступа к данным

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

2FA менеджер

Дополнительный уровень аутентификации пользователей с помощью комбинации двух различных компонентов

МЕНЕДЖЕР ПАРОЛЕЙ

Устраняет риски кражи учетной записи, централизовано управляя паролями системы и администратора

МЕНЕДЖЕР ПАРОЛЕЙ

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 надежное и безопасное
- Мультиаккаунт подключение к разным устройствам с 1 учетной записью
- 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.

МЕНЕДЖЕР ПАРОЛЕЙ: ПРОБЛЕМАТИКА

- Простые пароли
- Отслеживание паролей, кто использовал, когда и почему
- Использование одного и того же пароля для многих систем
- Приложения хранят учетные данные в конфигурационных файлах, БД или исходных кодах
- Обмен паролями среди коллег
- Не изменяются пароли через равные промежутки времени

МЕНЕДЖЕР ПАРОЛЕЙ: 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

МЕНЕДЖЕР СЕССИЙ

Мониторинг и контроль
всех привилегированных сеансов

МЕНЕДЖЕР СЕССИЙ

Протоколы

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

Поддерживаемые устройства

- MS Windows: любая версия
- Linux/Unix: Debian, Ubuntu, Red Hat, CentOS, MacOS и др.
- Оборудование сети: роутеры, коммутаторы и др. любого вендора
- Любое другое hardware/software с заявленными протоколами

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

МЕНЕДЖЕР СЕССИЙ: ПРОБЛЕМАТИКА

- Сложность управления доступом для сотен пользователей, подключающихся к тысячам систем
- Отсутствие центральной точки контроля доступа для критически важных систем
- Предоставление пользователям больше привилегий, чем им 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

МЕНЕДЖЕР СЕССИЙ: 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

2FA МЕНЕДЖЕР

Дополнительный уровень аутентификации

ДВУХФАКТОРНАЯ АВТОРИЗАЦИЯ

Каналы

e-mail

sms

Функциональность

Фактор:
online OTP

Фактор:
геолокация
пользователя

2 FA
для сторонних
решений

Настраиваемая
интеграция

Размерность

2FA МЕНЕДЖЕР: 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

2FA МЕНЕДЖЕР: 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

TACACS+ МЕНЕДЖЕР

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

TACACS+ МЕНЕДЖЕР ДОСТУПА

Протокол

TACACS+

Поддерживаемые устройства

Cisco, Juniper Networks, Huawei, ZTE, Nokia, Ericsson, Fortinet, Citrix, F5, McAfee, Paloalto Networks, & Custom

Размерность

Функциональность

- AAA-система
- SSO аутентификация
- Авторизация по настраиваемым политикам
- Для любого оборудования
- Логирование и быстрый поиск
- Долгосрочное хранение логов
- Поддержка сети любого объема
- Замена любой AAA-системы

TACACS+ МЕНЕДЖЕР: ПРОБЛЕМАТИКА

- Тысячи устаревших сетевых элементов, которыми нужно управлять с помощью протоколов TACACS+
- Сложность устаревших моделей определения политики TACACS+
- Несколько серверов TACACS+ для разных отделов в пределах одного предприятия
- Состояние окончания срока службы Cisco ACS

TACACS+ МЕНЕДЖЕР: 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

МЕНЕДЖЕР ДОСТУПА К ДАННЫМ

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

МЕНЕДЖЕР ДОСТУПА К ДАННЫМ

Поддерживаемые базы данных

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

Размерность

Функциональность

- SSO
- Политики SQL-запросов
- Firewall – доступа к данным
- Запись запросов
- Логирование и быстрый поиск
- Долгосрочное хранение логов
- Соответствие законодательству

МЕНЕДЖЕР ДОСТУПА К ДАННЫМ: ПРОБЛЕМАТИКА

- Администраторы баз данных с высоким уровнем привилегий могут просматривать или 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

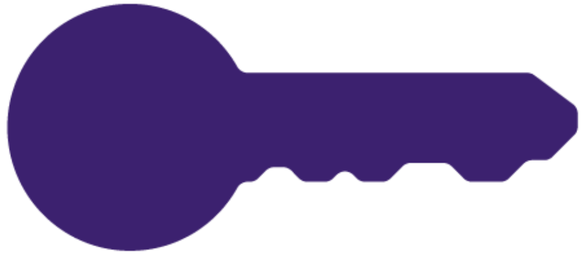
МЕНЕДЖЕР ДОСТУПА К ДАННЫМ: РЕШЕНИЕ

- 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

INFRASCOPE

О продукте

КЛЮЧЕВЫЕ ПРЕИМУЩЕСТВА



1. **Безагентское подключение**
   Без агентов на конечных точках
2. **Комплексность**
   Широкий диапазон поддержки протоколов
3. **Централизация**
   Единое средство видимости и управления всеми привилегированными сеансами
4. **Предотвращение в реальном времени**
   Предотвращение вредоносных действий до их возникновения
5. **Быстрота развертывания**
   Самый быстрый в развертывании
6. **Прозрачность**
   Прозрачное применение политик безопасности
7. **Модульность**
   Добавление модулей по запросу
8. **Непрерывность**
   Администраторы продолжают использовать собственные клиентские приложения
9. **Масштабируемость**
   Поддержка десятков тысяч конечных точек со стандартным сервером

АРХИТЕКТУРА РЕШЕНИЯ

Программное обеспечение

vmware

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»

*может быть установлен на другом гипервизоре

РАСШИРЕННЫЕ ВОЗМОЖНОСТИ

Контроллер

Для крупных распределенных систем

Контроль инцидентов

Централизованное хранилище данных в PostgreSQL

Централизованный быстрый поиск

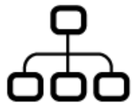
Централизованная репликация и синхронизация

Изолированная среда исполнения

Изоляция

Управление привилегированными сессиями

Секретное хранилище



Разделение пользователей и устройств

КОНТАКТЫ

121096 г. Москва, ул. Василисы Кожиной,
д. 1, корп. 1, этаж 7

ТЕЛ +7 (495) 269-29-59
ПОЧТА sales@ngrsoftlab.ru
САЙТ ngrsoftlab.ru