Обзор решения Infrascope: контроль привилегированного доступа

Статистика показывает, что в 43% нарушений данных были вовлечены внутренние пользователи, половина из них действовала преднамеренно. Привилегированные учетные записи являются главным приоритетом при мониторинге и контроле доступа на предприятии. Поэтому решения класса PAM (Privileged Access Management) — универсальный инструмент для их защиты. Он помогает снизить риски при использовании сервисных и неперсонифицированных учетных записей конечных устройств (маршрутизаторов и др). PAM-решения фокусируются на контроле и защите внутренней ИТ-среды организации, в том числе при использовании аутсорсинговых услуг и удаленного доступа.

Infrascope — PAM-решение с широким диапазоном функций «из коробки», которое помогает предприятиям создать гибкую, централизованную, многоуровневую архитектуру защиты от инсайдерских угроз и компрометации учетных записей.

Функциональные возможности

Infrascope предоставляет набор функциональных модулей, расширяющих возможности классического PAM:

- **Динамический диспетчер паролей** — централизованное безопасное хранилище паролей, позволяющее предотвратить кражу или несанкционированный обмен. Пользователи используют учетные записи Infrascope, а система самостоятельно обновляет пароли от учетных записей в целевых системах. Технология позволяет дополнительно управлять учетными записями приложений (AAPM), обеспечивая их выдачу через API и производить автоматическую ротацию паролей для общих и сервисных учетных записей без необходимости их перенастройки (SAPM).
- **Менеджер сессий** контролирует и проверяет зашифрованные сеансы пользователя. Менеджер сессий работает как шлюз между пользователями и целевыми конечными точками. Все сессии логируются в т.ч. с записью видео. На все сессии может быть применена политика, ограничивающая действия плоть до запрета ввода конкретных команд, выполнения действий, запуска приложений и пр.
- **Двухфакторная аутентификация** позволяет использовать одноразовые пароли, отправляемые по электронной почте, СМС (требует приобретения отдельного сервиса) или с использованием сторонних публичных сервисов аутентификации. Двухфакторная аутентификация гарантирует, что учетная запись действительно принадлежит лицу, осуществляющему подключение, позволяет быстро восстановить доступ в случае утери пароля.
- **TACACS+ менеджер** — модуль поддержки и управления аутентификацией для администрирования сетевых устройств по протоколам TACACS и RADIUS. Поддерживает SSO – сквозной вход без необходимости многократного ввода одних и тех же учетных данных.
- **Менеджер доступа к данным** позволяет отслеживать и проверять зашифрованные сеансы администратора базы данных. Модуль обеспечивает функции разграничения доступа на уровне БД и поддерживает маскирование чувствительных данных. Доступно простое управление сеансами к SQL-like и нереляционным СУБД наиболее популярных производителей.

Система предоставляет возможности контроля за действиями поставщиков услуг, администраторами ИТ-инфраструктуры и обеспечивает выполнение требований стандартов ИБ (ГОСТ 57580 — Безопасность финансовых (банковских) операций, GDPR, PCI DSS, ISO 27002 и др.)

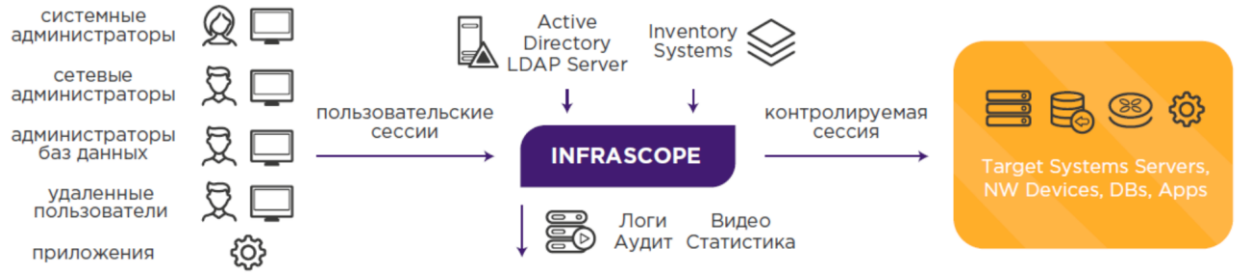

Рис. 1. Схема работы Infrascope

Технические характеристики

Система поддерживает вертикальное и горизонтальное масштабирование, применение многонодовых кластерных инсталляций active-active.

Рассчитана на стабильную одновременную (конкурентную) работу пользователей без ограничений по количеству.

Сценарии применения

Рис 2. Функции применения Infrascope

Менеджер паролей

Устраняет риск кражи учетной записи, централизовано управляя паролями системы и администратора.

Пользователи проверяют учетные данные из динамического диспетчера паролей Infrascope, а затем используют его для подключения к целевой конечной точке для выполнения своих задач. Индексированное логирование и журналы аудита генерируются согласно требованиям законодательства по безопасности.

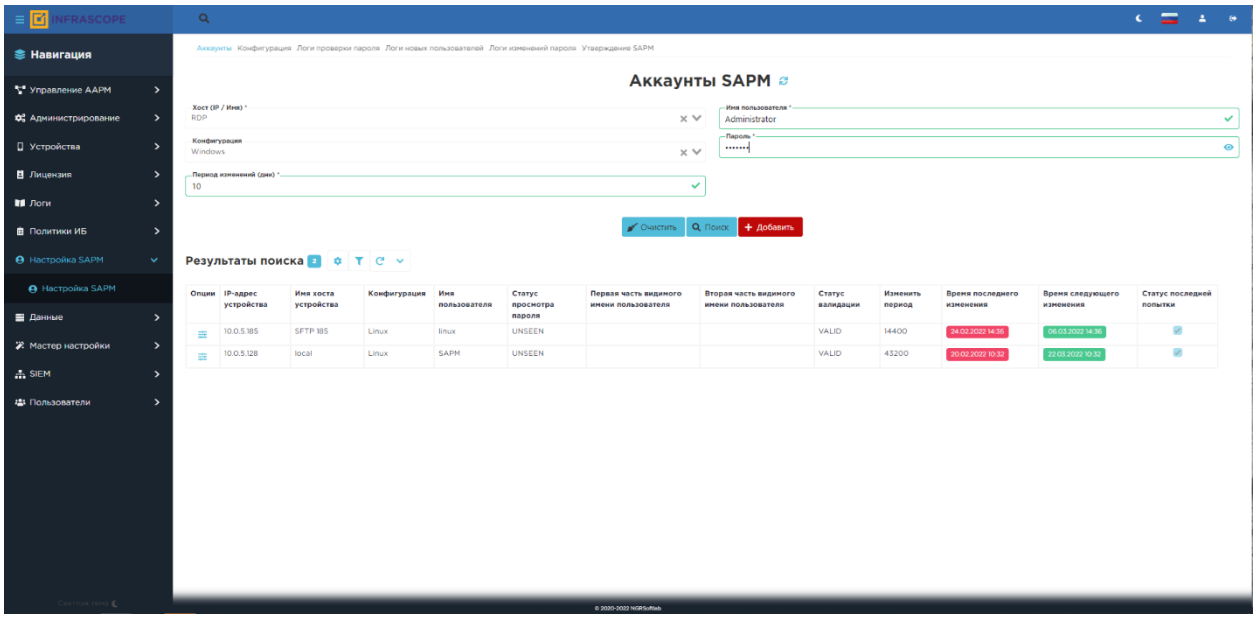

Рис.3. Менеджер паролей

Менеджер сессий

Менеджер сессий Infrascope контролирует и проверяет зашифрованные сеансы пользователя. Менеджер сессий работает как шлюз между пользователями и целевыми конечными точками.

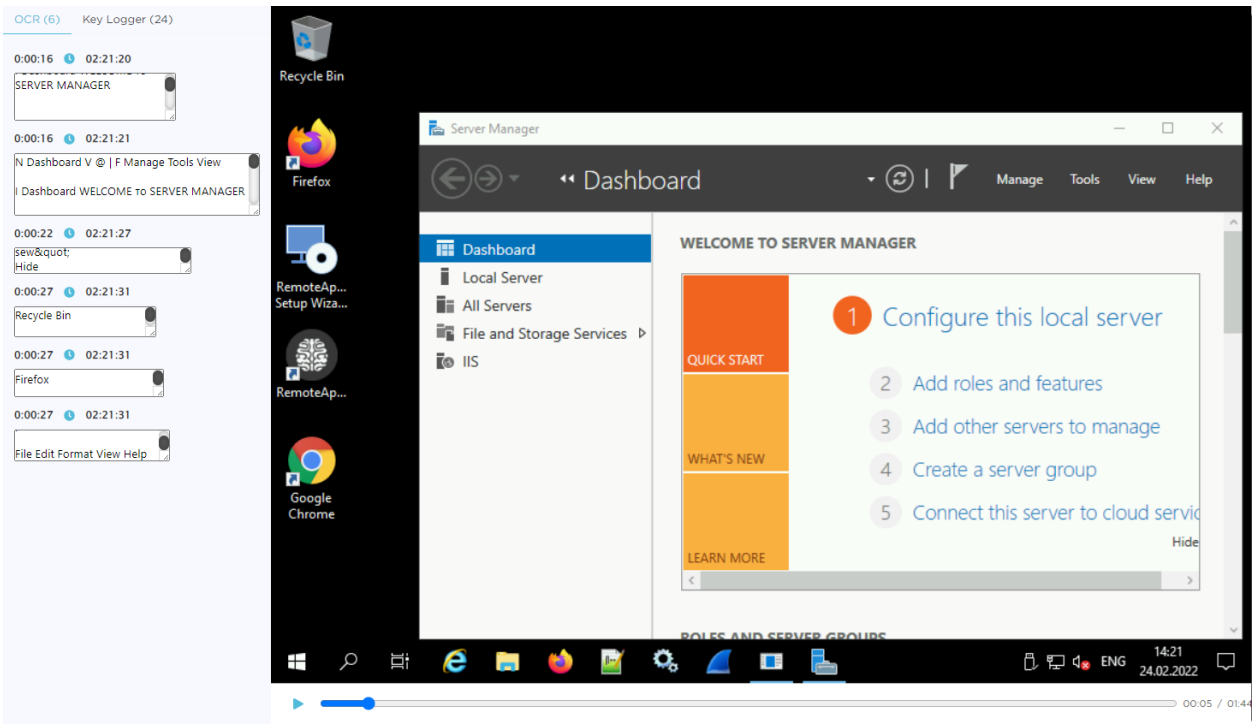

Рис. 4. Менеджер сессий

2FA-менеджер — дополнительный уровень аутентификации

Двухфакторная авторизация Infrascope — дополнительный уровень аутентификации с помощью комбинации двух различных компонентов. Дополнительный код (одноразовый пароль), полученный по электронной почте или с использованием внешнего сервиса одноразовых паролей, необходимо ввести во время аутентификации, что послужит подтверждением личности пользователя. Автономная генерация кода в режиме реального времени поддерживается с помощью сильного генератора токенов.

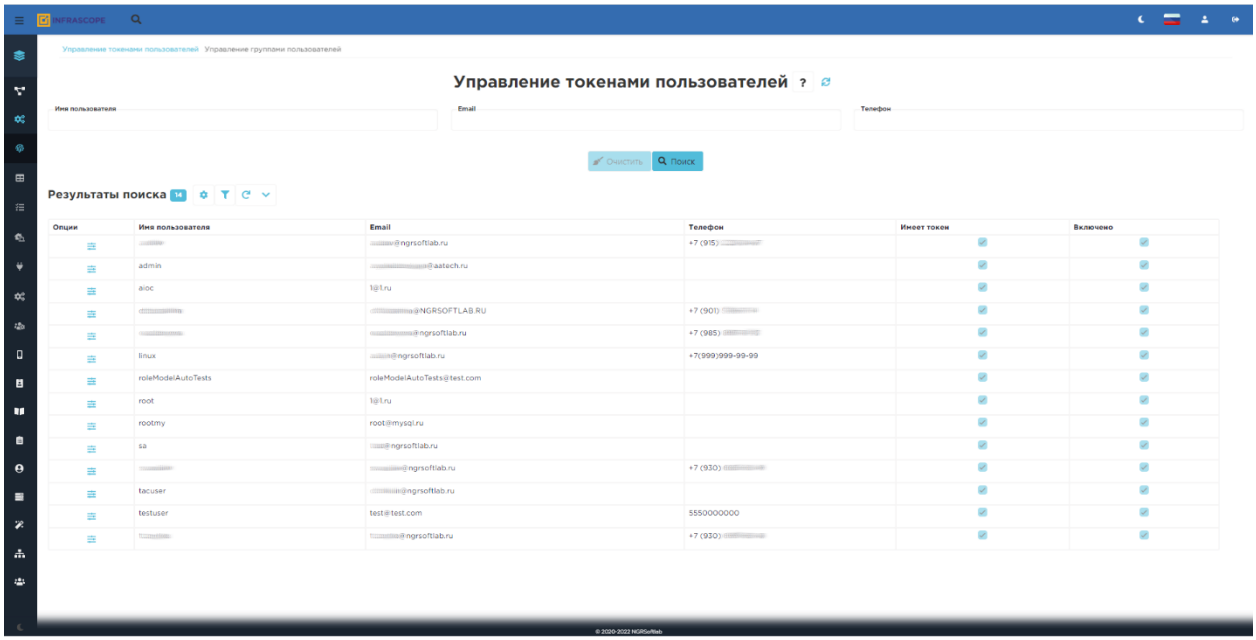

Рис. 5. Двухфакторная аутентификация

TACACS+ менеджер

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

Каждая попытка аутентификации и запуска команд пользователем передается с устройства/сервера в TACACS+ менеджер Infrascope, который позволяет централизованно управлять и применять многие функции, включая SSO – единый вход, принудительное применение наименьших политик, ведение журнала, мультиарендность (Multitenancy).

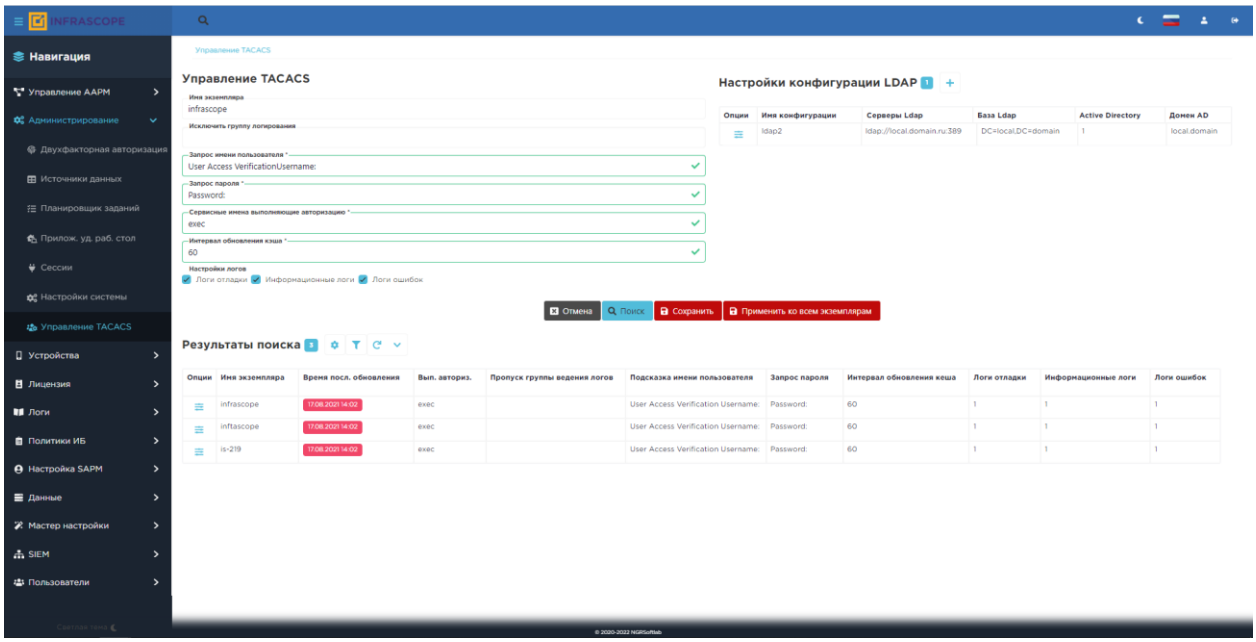

Рис. 6. TACACS+ менеджер

Менеджер доступа к данным

Менеджер доступа к данным Infrascope обеспечивает и контролирует привилегированный доступ к базам данных, предоставляя функцию динамического маскирования для предотвращения доступа к конфиденциальным данным.

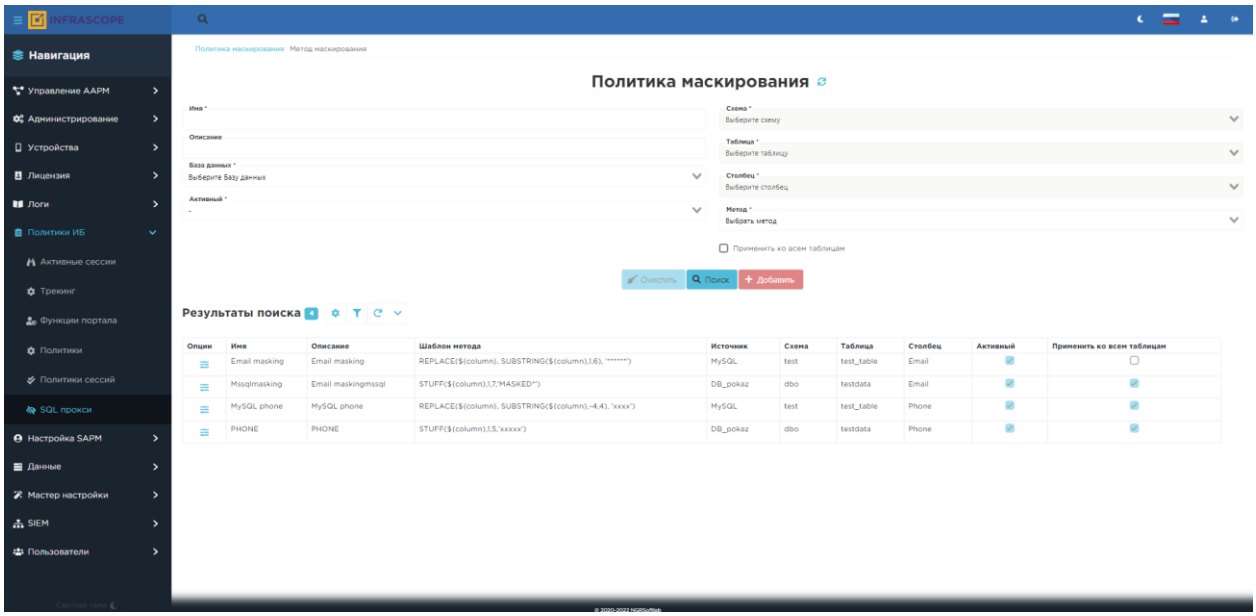

Рис. 7. Менеджер доступа к данным

Состав и архитектура решения

Инфраскоп имеет модульную и интеграционную архитектуру с поддержкой широкого спектра протоколов и функций на одной платформе.

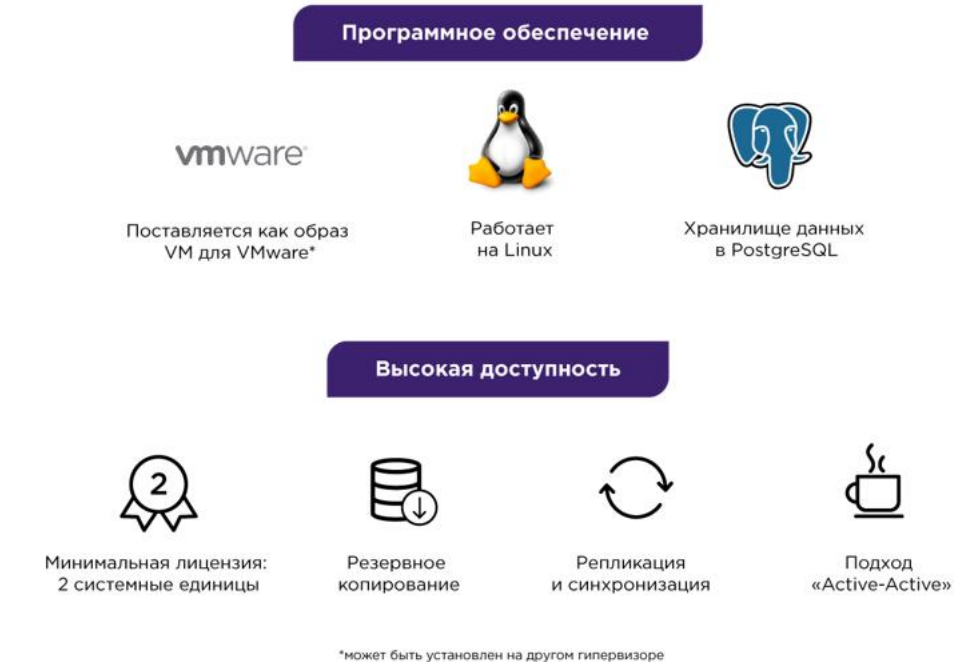

Рис. 8. Архитектурные особенности Infrascope

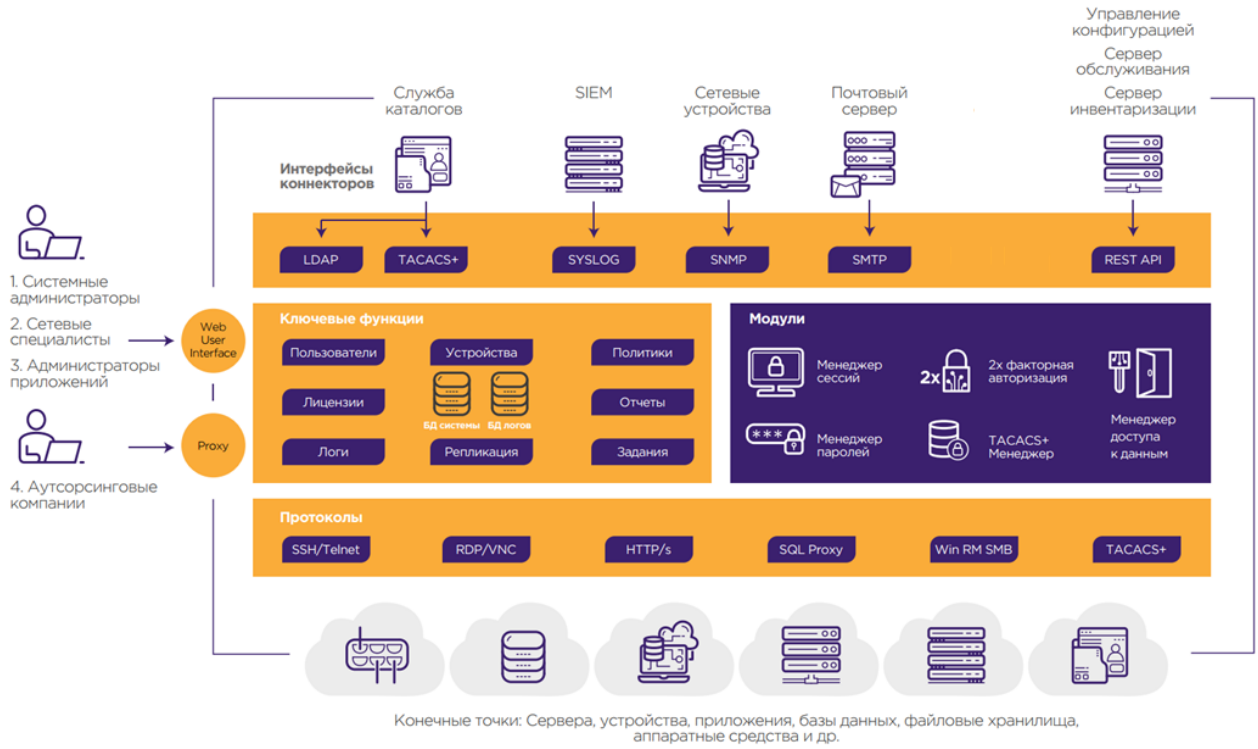

Рис. 9. Архитектура Infrascope

Пользователи используют веб-интерфейс Infrascope для:
- веб-подключения удаленного рабочего стола к серверу Windows;
- веб-подключения CLI к сетевому устройству;
- проверки пароля из секретного хранилища и т.д.

Также возможно подключение с помощью собственных клиентов вместо веб-интерфейса. Например, пользователи могут использовать:
- собственный CLI (Putty, SecretCRT);
- Windows-приложение удаленного рабочего стола;
- SQL-клиента (TOAD, DataGrid, Navicat, и т.д.);
- приложения для прямого подключения к Infrascope прокси-сервисов по SSH/Telnet, RDP и SQL.

Системные требования

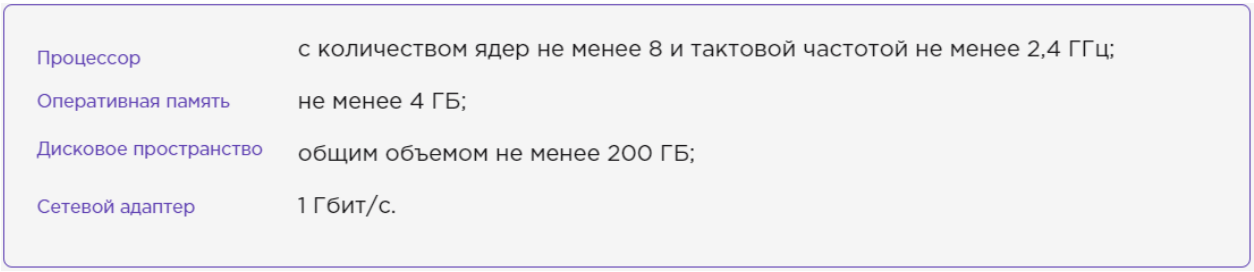

Рис. 10. Минимальные системные требования Infrascope

Внедрение включает в себя: развертывание образа, первоначальную настройку, последующее подключение контролируемых устройств, заведение пользователей системы и контролируемых устройств, настройку политик.

Варианты поставки и лицензирование

Имеются постоянные (перманентные) и временные лицензии. Лицензируется как с использованием «бандлов» (наборов модулей и количественных ограничений к ним), так и в режиме конструктора. Основные лицензируемые характеристики:

- Используемые модули (контролируемые протоколы).
- Количество конечных устройств или конкурентных пользователей.
- Дополнительные возможности модулей, такие как: поддержка внешних сервисов многофакторной аутентификации и пр.

Система поставляется как отдельный OVA-контейнер для автоматизированного развертывания в любой среде виртуализации. Подтвержденными (протестированными) являются VMware и KVM.

Интеграция с другими решениями

Поддерживаются любые решения по следующим протоколам:

- RDP (Windows), SSH (любые *nix), VNC (Linux GUI), Oracle TNS, MySQL, Cassandra, MS SQL, Hive, Teradata, Postgresql.
- Интеграция с SIEM по syslog и электронной почтой по SMTP для отправки событий и уведомлений, а также отправки одноразовых паролей.
- Поддержка внешних сервисов многофакторной аутентификации для использования одноразовых паролей.
- Authy, Duo Mobile, LastPass Authenticator, Microsoft Authenticator, Google Authenticator, Яндекс Ключ.
- Интеграция со службами каталогов в т.ч. MS AD или любой другой, поддерживающей LDAP\LDAPS для импорта пользователей и устройств.

Для любой компании важно ответственно подходить к защите данных. Ведь доступ злоумышленников к привилегированному аккаунту угрожает распространением вирусного кода по всей инфраструктуре, утечкой конфиденциальной информации, а также большими потерями для бизнеса.

Infrascope включен в реестр отечественного ПО. Это проверенное решение сокращает время настройки контроля доступа привилегированных пользователей примерно на 80% по сравнению с другими и может масштабироваться для поддержки десятков тысяч пользователей и учетных записей, миллионов устройств и конечных точек, а также миллиардов комбинаций аутентификации.