SOLAR SAFEINSPECT

Полнофункциональная PAM-система

PAM (PRIVILEGED ACCESS MANGEMENT) — ТЕХНОЛОГИЯ, ОБЕСПЕЧИВАЮЩАЯ БЕЗОПАСНОСТЬ СЕССИЙ ПРИВИЛЕГИРОВАННЫХ ПОЛЬЗОВАТЕЛЕЙ, ЗАЩИТУ ПОДКЛЮЧЕНИЙ К КРИТИЧЕСКИМ СИСТЕМАМ КОМПАНИИ И МИНИМИЗИРУЮЩАЯ РИСКИ УТЕЧКИ УЧЕТНЫХ ЗАПИСЕЙ С РАСШИРЕННЫМИ ПРАВАМИ.

58

раз в год в среднем компании сталкиваются с проблемами привилегированного доступа[1]

71%

уязвимостей во внутренних сетях связаны с использованием пользователями слабых паролей[2]

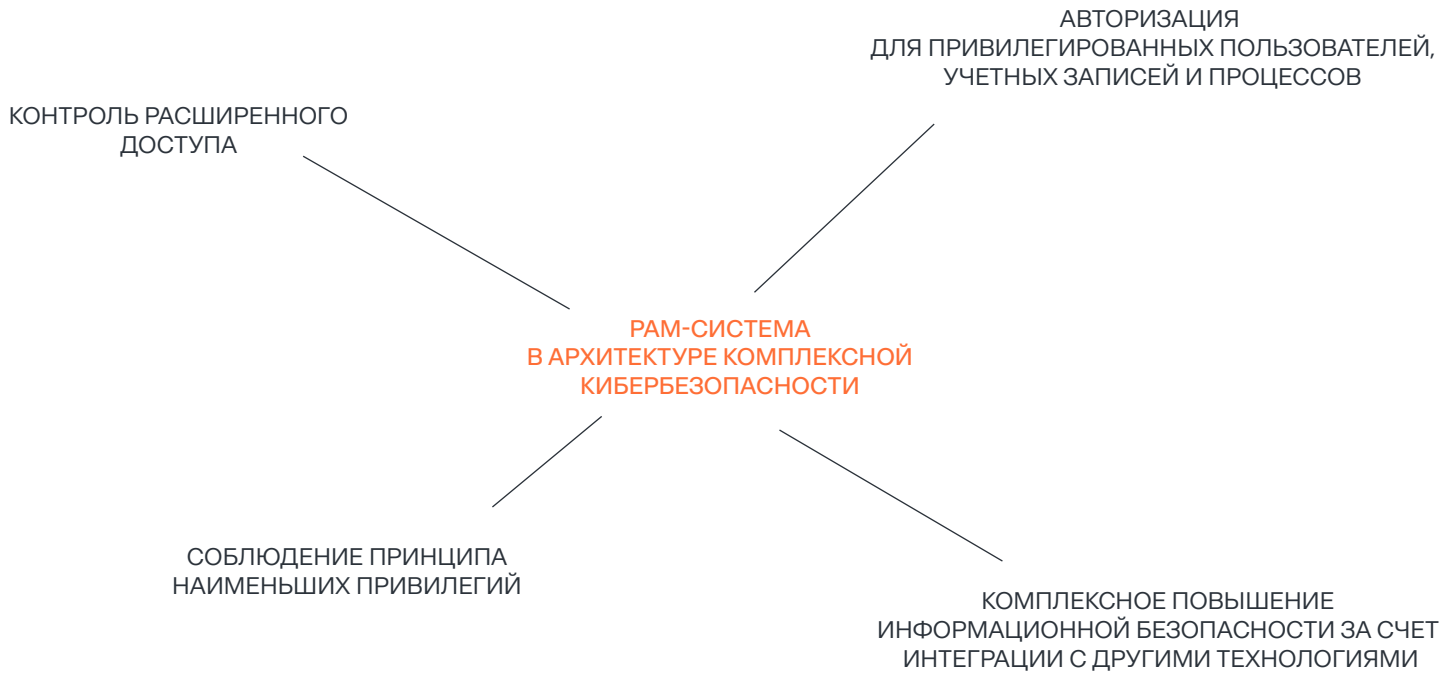
5,5 МЛН РУБ.

средний ущерб от инцидентов, связанных с утечкой информации[3]

[1] По данным исследования ключевых уязвимостей информационных систем российских компаний, март 2023

[2] По данным внутреннего рыночного исследования «СОЛАР», декабрь 2023

[3] По данным исследования «СОЛАР», сентябрь 2023, выборка из 79 компаний крупного коммерческого и государственного секторов



Ключевые угрозы

Скачивание запрещенного контента

Изменение логов и журналов действий

Изменение конфигураций информационных систем

Обход политики безопасности

Несанкциони-рованные финансовые операции

Использование обезличенных учетных записей

Привилегированные пользователи — кто это?

РЯДОВЫЕ ПОЛЬЗОВАТЕЛИ

Уровень риска

Низкий и (редко) средний

К чему имеют доступ

- Бизнес-приложения и системы
- ПДн, конфиденциальная коммерческая информация

Вероятный ущерб

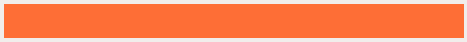
- Утечка коммерческой информации
- Изменение настроек безопасности (на рабочем устройстве)
- Установка мелких вредоносов (расширения для браузера, плагины для MS Office и т. д.)

Тип прав

Базовые права на чтение, изменение или удаление информации в ИС

ПРИВИЛЕГИРОВАННЫЕ ПОЛЬЗОВАТЕЛИ

Уровень риска



Высокий и критический

К чему имеют доступ

- Сетевая инфраструктура
- СЗИ, ВМ, БД
- Бизнес-приложения (администрирование)

Вероятный ущерб

- Отключение СЗИ, систем безопасности и мониторинга, изменение политик безопасности
- Внесение изменений в конфигурацию целевых серверов
- Реализация атак злоумышленников
- Крупные утечки информации

Тип прав

Расширенный доступ к критически важным элементам инфраструктуры

Кто обладает привилегированным доступом?

ВНУТРЕННИЕ СОТРУДНИКИ

- Системные администраторы, техподдержка
- Бизнес-пользователи с расширенным доступом (владельцы систем)
- Операторы баз данных

ВНЕШНИЕ СОТРУДНИКИ

- Внешние поставщики ИТ-услуг и компонентов
- Интеграторы, вендоры
- Аутсорсеры
- Аудиторы

Мы предлагаем эффективное управление и контроль безопасной работы

01

Изолирование (проксирование) привилегированных сессий

02

Мониторинг работы в реальном времени с возможностью прерывания сессии

03

Запись сеансов работы пользователей с расширенными правами

04

Гибкие возможности анализа записанных сессий

05

Обнаружение всех пользователей с расширенными полномочиями

06

Гранулированный доступ к комплексу программно-аппаратных решений на базе политик безопасности

07

Возможность хранения записей сессий привилегированных пользователей

08

Подстановка и сокрытие учетных данных привилегированных пользователей

Основные преимущества решения

КООРДИНАЦИЯ ПРИВИЛЕГИРОВАННОГО ДОСТУПА

Гибкая и оперативная организация доступа под любые задачи: постоянно, согласно действующему расписанию, единовременно или повторно, по группам доступных активов и по определенным операциям внутри этих активов

ПРОСТОТА РАЗВЕРТЫВАНИЯ

Первичное развертывание и настройка решения при выборе Virtual Appliance максимум за 20 минут. Первые результаты мониторинга могут быть получены через 2 часа

3 СЦЕНАРИЯ ИНТЕГРАЦИИ СИСТЕМЫ

Интеграция системы в режимах маршрутизатора и сетевого моста позволяет организовать прозрачное подключение пользователя.
В режиме Бастион пользователь проходит явную авторизацию через дополнительное окно ввода учетных данных

ГИБКОЕ ВСТРАИВАНИЕ В ИНФРАСТРУКТУРУ

Возможность установить программный комплекс в распределенной инфраструктуре, в любых местах корпоративной ИТ-среды — без установки агентов на рабочих местах

НАДЕЖНОЕ И БЕЗОПАСНОЕ ХРАНЕНИЕ ИНФОРМАЦИИ

Сведения, записанные системой, компактно упакованы для хранения. Периоды простоя не требуют дополнительного места. База данных — под защитой шифрования

СЕРТИФИЦИРОВАННОЕ ОТЕЧЕСТВЕННОЕ РЕШЕНИЕ

Solar SafeInspect сертифицирован ФСТЭК России по 4-му уровню доверия, внесен в Единый реестр отечественного ПО и подходит для импортозамещения

4 шага к безопасности

1

ОБНАРУЖЕНИЕ

Фиксирование на всех критически важных ИТ-ресурсах привилегированных учетных записей и их взаимосвязей на оборудовании и в ПО

2

ДЕЛЕГИРОВАНИЕ

Обеспечение доступа к привилегированным УЗ только уполномоченному персоналу, в строго отведенное время, с обязательным учетом целей доступа и соблюдением принципа наименьших привилегий

3

ВЫПОЛНЕНИЕ

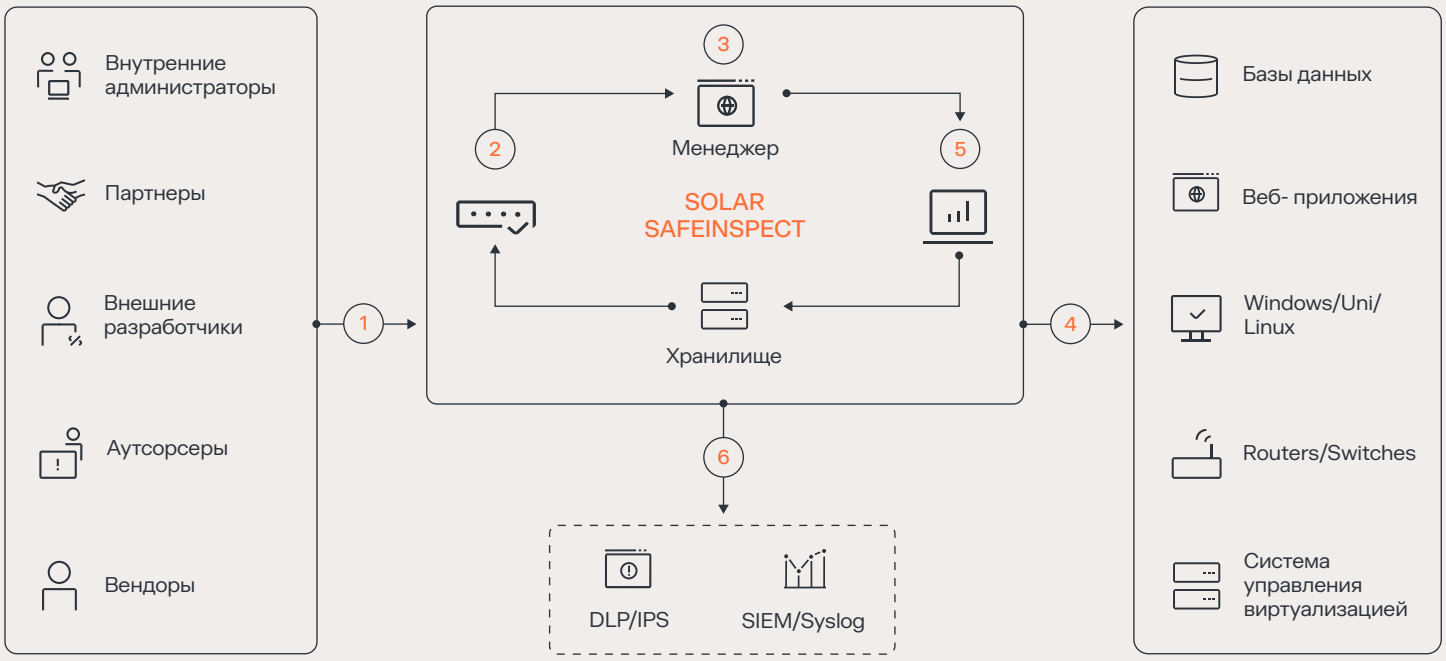
Принудительное применение правил разнообразия и частоты смены паролей с синхронизацией изменений на всех ИТ-ресурсах

4

КОНТРОЛЬ

Организация аудита: кто, с какой целью и как долго пользуется привилегированным доступом. Извещение ответственных лиц о подозрительной деятельности пользователей

Архитектура решения



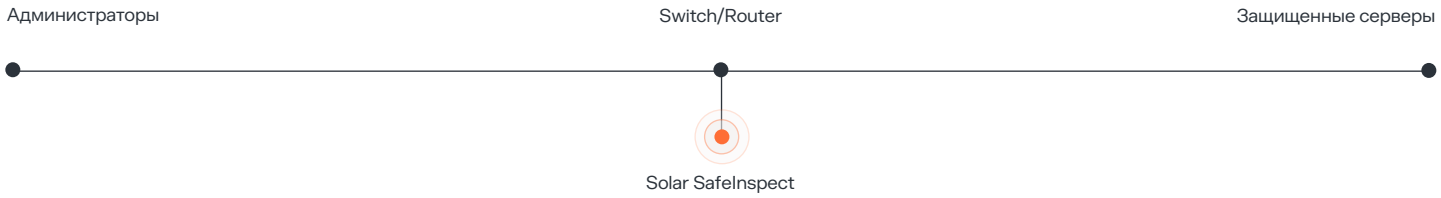
1 Подключение
2 Идентификация/ Аутентификация
3 Проверка на доступ к ресурсам/ Сопоставление
4 Подключение к ИС
5 Сохранение записи сессий
6 Взаимодействие со смежными системами

Три режима работы

БАСТИОН

В этом режиме Solar SafeInspect выполняет роль прокси-сервера и обрабатывает весь трафик запросов к серверам. Пользователь и целевые серверы при этом находятся в сети организации.

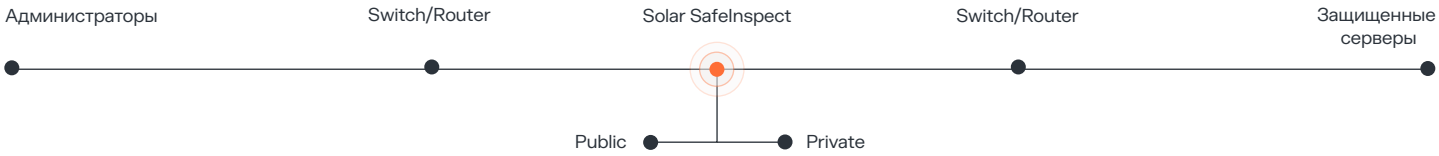
При обращении к запрашиваемому ресурсу Solar SafeInspect подключается к нему по защищенному протоколу.



СЕТЕВОЙ МОСТ

Схема предназначена для контроля доступа сотрудников компании. Solar SafeInspect устанавливается«в разрыв», то есть все соединения с внутренними серверами проходят через PAM-систему на канальном уровне.

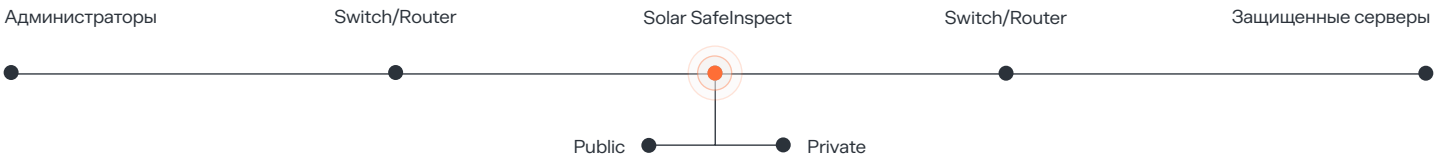
В этом режиме авторизация происходит незаметно для пользователя.



МАРШРУТИЗАТОР

При таком режиме работы системы администраторы и серверы находятся в разных сетях. При этом Solar SafeInspect также устанавливается «в разрыв» — соединения с целевыми серверами маршрутизируются на PAM-систему.

В этом режиме авторизация происходит незаметно для пользователя.



Функциональные возможности Solar SafeInspect

АУТЕНТИФИКАЦИЯ И АВТОРИЗАЦИЯ

Предоставление доступа к привилегированным учетным записям только после надежной аутентификации

ГРАНУЛИРОВАННЫЙ ДОСТУП

Только для выбранных сотрудников к конкретным ресурсам и учетным записям на определенное время

УПРАВЛЕНИЕ ПАРОЛЯМИ

Изменение по расписанию и надежное хранение

ЗАПИСЬ СЕАНСОВ ПРИВИЛЕГИРОВАННЫХ ПОЛЬЗОВАТЕЛЕЙ

Возможность индексации, поиск по ключевым словам

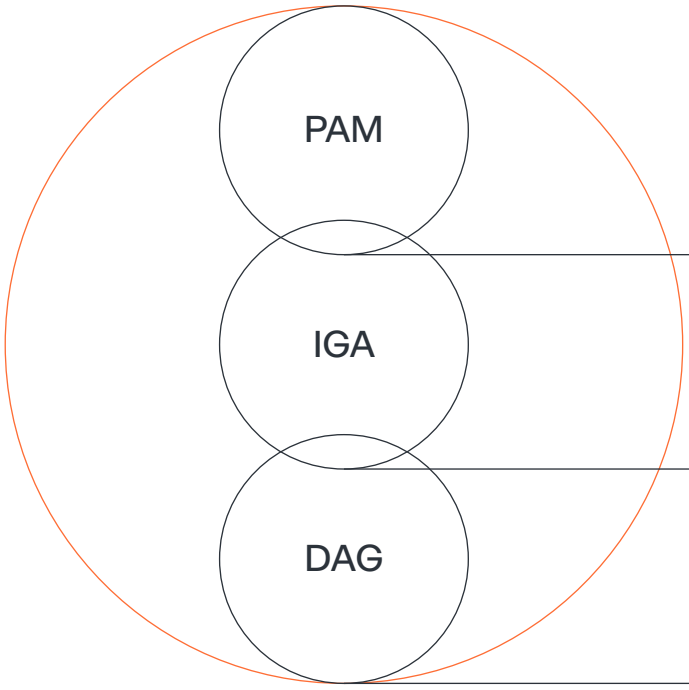
РУЧНОЙ ИЛИ АВТОМАТИЧЕСКИЙ ОБРЫВ СЕАНСА

Возможность защиты в случае обнаружения подозрительной активности

КОНТРОЛЬ ШИРОКОГО СПЕКТРА ПРОТОКОЛОВ ПЕРЕДАЧИ ДАННЫХ

RDP (RDS, Remote APP), SSH, SCP, Telnet/Telnets, HTTP/HTTPs, SFTP, TCP, TLS, VNC и др.

Возможности интеграции — комплексный подход к безопасности



Фокус на управлении и мониторинге привилегированных пользователей для предотвращения несанкционированного доступа и злоупотреблений

Централизованная платформа управления учетными записями и правами доступа пользователей к информационным ресурсам, единый каталог пользователей

Мониторинг и контроль доступа к неструктурированным данным в покое

SOLAR

W: RT-SOLAR.RU
W: RT.RU

T +7 (499) 755-07-70
E solar@rt-solar.ru

Центральный офис, 125009,
Москва, Никитский переулок, 7с1