ZECURION

Привилегированные пользователи: скрытая угроза корпоративной безопасности

Артём Смирнов

Проблемы привилегированных аккаунтов

01 Без них нельзя обойтись

Ни один бизнес не обходится без использования таких учётных записей. Их нужно контролировать

02 Совместное использование

Один и тот же привилегированный аккаунт используется несколькими пользователями

03 Широкий доступ к важным данным

Привилегированные учётные записи могут передавать сотрудникам, не имеющих таких прав доступа

04 Невозможно отследить

Нет возможности отследить кто именно их использует, и для каких целей

Что делать?

- Обнаружить все привилегированные учетные записи
- Начать управлять доступом привилегированных пользователей
- Изолировать и контролировать доступ к серверам, БД, виртуальным платформам
- Расследовать инциденты и выявлять недобросовестных пользователей

Типичные задачи PAM

Предотвращать злонамеренную манипуляцию данными

Создание и управление политиками доступа к администрируемым ИТ системам

Защита от сокрытия действий и очистки системных журналов

Централизованное хранение данных по сессиям пользователей

Централизованное управление учетными записями пользователей

Аудит сессий пользователей, своевременная реакция и запрет

Каким компаниям необходим PAM?

С численностью ИТ-персонала от 5 человек

С количеством объектов с различными паролями от 10

С необходимостью расследования действий админов

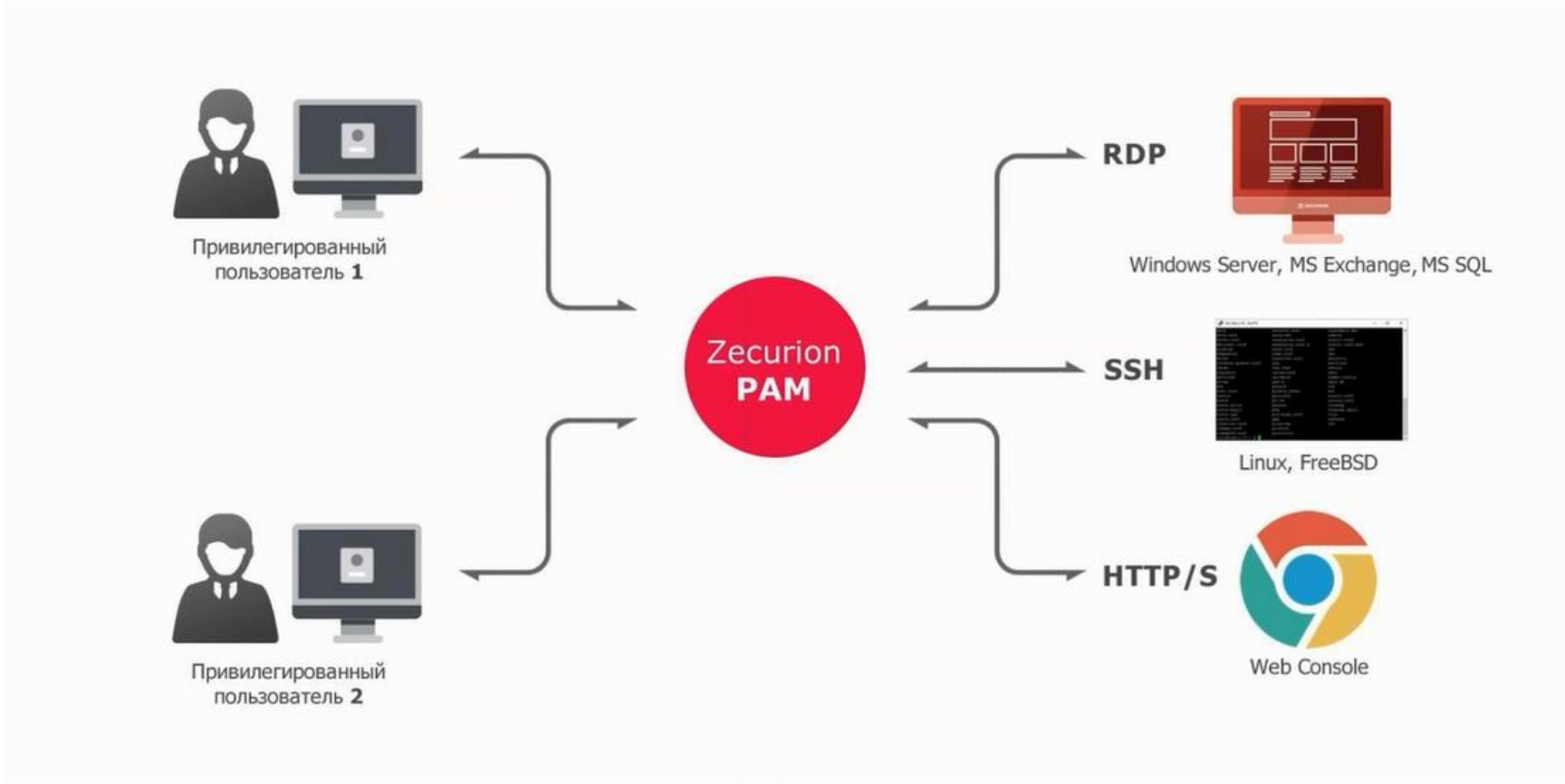
Наличие ИТ систем требующих технической поддержки от вендора или интегратора

Пользующиеся услугами ИТ-аутсорсинга

Предоставляющие доступ сторонним организациям/ подрядчикам

Возможности Zecurion PAM

Как работает Zecurion PAM



Сценарии использования системы

Мониторинг

Мониторинг соединений со всеми объектами сети.

Просмотр действия привилегированных пользователей в режиме онлайн.

Архив

Ведение архива сессии пользователей.

Хранение истории как в графическом варианте (актуально для RDP), так и в текстовом (командная строка через SSH).

Расследование

Фиксация всех атрибутов сессий

Поиск и просмотр данных в ходе расследования инцидентов и выявления недобросовестных сотрудников

Мониторинг действий

Возможности

- Просмотр действий привилегированных пользователей в режиме онлайн
- Гибкие настройки мониторинга по пользователям и группам
- Возможность просмотра действий пользователей с любой клиентской ОС

Архивирование информации

Возможности

- Запись всех действий и видеофиксация рабочего стола пользователей
- Быстрый поиск информации в архиве
- Построение наглядных графиков и полная статистика действий пользователей

Расследование инцидентов

Возможности

- Предоставление полной детализированной статистики о действиях привилегированных пользователей
- Архив всех действий и операций удалённого доступа к системам
- Оперативный поиск информации о сеансах в архиве

Почему Zecurion PAM?

Гибкое управление доступом

Платформонезависимость

Простые установка и настройка

Современная консоль управления

Удобные отчёты

Агентонезависимая технология

О компании Zecurion

- Фокус — защита информации от утечек (DLP) и от угроз со стороны привилегированных пользователей (PAM)
- Продукты Zecurion входят в рейтинг лучших мировых DLP-решений (Gartner) и реестр отечественного ПО (Минсвязи)
- Более 10 000 заказчиков и более 150 партнёров
- Лицензии и сертификаты ФСБ, ФСТЭК, Министерства Обороны РФ
- Компания входит в состав АРПП «Отечественный софт»

Мы защищаем


ТЕХНО
СИЛА


Allianz


МИНИСТЕРСТВО
ФИНАНСОВ РФ


СБЕРБАНК


МОРТОН


БАШНЕФТЬ


СВЯЗНОЙ


РОСНЕФТЬ


ВТБ
ПЕНСИОННЫЙ
ФОНД


МИНИСТЕРСТВО ОБОРОНЫ
РОССИЙСКОЙ ФЕДЕРАЦИИ


ТУПОЛЕВ
Открытое
акционерное
общество


1921
РОСГОССТРАХ


МОСКОВСКИЙ
КРЕДИТНЫЙ
БАНК


Ростелеком


ФОСАГРО


МЭС
МОСЭНЕРГОСБЫТ

Итоги

Решаемые задачи

- Организация централизованного контроля доступа и действий привилегированных пользователей с корпоративными ИТ системами
- Создание независимого от ИТ центра аудита работы администраторов корпоративных системам

Основные функции

- Централизованное управление учетными записями и политиками разрешения доступа пользователей и администраторов
- Сокрытие исходных паролей администрируемых систем
- Единый архив событий и инцидентов для контроля и расследований

Остались вопросы?
Задайте их специалистам
на нашем стенде!

ZECURION