Рутокен PAM

Рутокен PAM — программный комплекс для управления доступом к привилегированным учетным записям. Рутокен PAM защищает пароли учетных записей администраторов и позволяет предоставлять пользователям только те права, которые необходимы для выполнения конкретных задач. Также он централизованно записывает все действия администраторов для последующего просмотра и анализа.

Рутокен PAM снижает риски финансовых и репутационных потерь.

Почему Рутокен PAM

Предоставлять пользователю привилегированный доступ к IT-инфраструктуре и информационным системам предприятия очень опасно. Данные могут быть скопированы, настройки изменены, а привилегированный доступ позволит пользователю «замести следы», уничтожив все записи в журналах. Если пароль системного администратора получает злоумышленник, последствия могут быть катастрофическими.

Бывает и такое, что проблемы возникают из-за ошибки самого администратора, а отсутствие постоянного контроля за его действиями не позволяет оперативно определить причину.

Рутокен PAM разработан, чтобы исключать утечки учетных данных администраторов и осуществлять контроль за их деятельностью. Он предназначен для управления доступом к привилегированным учетным записям и аудита действий сотрудников с повышенным уровнем доступа к ресурсам компании.

Программный комплекс решает проблему контроля доступа администраторов. При использовании Рутокен PAM пользователи с повышенным уровнем доступа подключаются к IT-инфраструктуре предприятия не напрямую. Рутокен PAM используется в качестве посредника. Благодаря этому обеспечивается надежная комплексная защита.

Преимущества

- **Двухфакторная аутентификация.** Организована возможность настройки двухфакторной аутентификация администраторов.
- **Управление паролями учетных записей администраторов.** Пароли скрываются от сотрудников и регулярно изменяются без их ведома.
- **Видео и текстовая запись сессий привилегированных пользователей.** Каждый сеанс доступа записывается и благодаря архиву записей можно понять, какие действия и кем были произведены в определенный момент времени.
- **Управление пользователями.** Централизованное управление пользователями с привилегированным доступом, проверка правильности выдачи прав.
- **Индивидуальные политики.** Возможность создавать индивидуальные политики доступа для решения конкретных задач.
- **Контроль за действиями администраторов.** Запись всех действий администраторов.
- **Отсутствие возможности использования учетных данных злоумышленниками.** Администраторы не знают данные аккаунтов, а, значит, злоумышленник не сможет их получить.

Возможности

Политики разрешения определяют, каким учетным записям в какой момент времени предоставлять доступ к определенным ресурсам. Также задаются параметры подключения, например, указывается, какие сессии необходимо записывать.

В хранилище привилегированных учетных данных находятся данные, необходимые для привилегированного доступа (логины, пароли, ключи SSH), к которому имеет доступ только сервер Рутокен PAM.

Подсистема записи сессий сохраняет взаимодействия привилегированных пользователей с IT-инфраструктурой. Ввод и вывод консоли в сессиях SSH, все запускаемые процессы, открываемые окна и ввод с клавиатуры для RDP подключений сохраняются в текстовом виде. Также может производиться запись для сессий RDP и SSH, снятие скриншотов и просмотр действий пользователей в режиме онлайн.

Журнальный сервер собирает все события Рутокен PAM, хранит их и обеспечивает их просмотр. Также есть возможность отправлять эти события в систему SIEM.

Консоль администратора — web-приложение для настройки, управления и аудита работы системы. Также оно позволяет администраторам Рутокен PAM просматривать активные сессии в реальном времени и при необходимости прекращать сеанс работы сотрудника.

Пользователи используют сервисы самообслуживания для просмотра доступных им учетных записей и запуска привилегированных сессий. Доступ к сервисам возможен с помощью специального приложения или web-приложения.

Модули доступа предоставляют механизмы открытия и записи привилегированных сессий. Подключение происходит через сервер доступа или SSH Proxy.

Подсистема управления учетными записями отвечает за создание привилегированных учетных записей на целевых ресурсах, проверку и смену паролей, ключей SSH.
Для этого в состав системы входят коннекторы для таких целевых систем, как Active Directory, Windows Server, а также Linux.

Характеристики

- Протоколы доступа: RDP, SSH, HTTP(s).
- Поддерживаемые типы учетных данных: имя пользователя + пароль, SSH-ключи.
- Поиск привилегированных учетных записей и управление паролями: Windows, Linux, Active Directory.
- Поддерживаемые каталоги пользователей: Active Directory.
- Технологии двухфакторной аутентификации: пароль + TOTP (программный генератор).
- Поддерживаемые типы записи сессий: текстовый лог, видеозапись, снимки экрана.
- Технологии удаленного доступа: Microsoft RDS, SSH Proxy.