



AFI Distribution
www.AFI-Distribution.ru

PAM

 **senhasegura**[®]

- Новый вендор в РФ и СНГ
- Комплексное PAM-решение
- Не поддерживает санкции ЕС и США

Проект Senhasegura

Аудитория и решения



senhasegura®

О компании

Senhasegura – разработчик ПО для управления привилегированными пользователями (PAM).

- Штаб-квартира в Бразилии
- Основана в 2001
- Высокие оценки решения в KuppingerCole и Gartner
- Лучшее решение по мнению пользователей Gartner “Peer Insight”

Подробнее: senhasegura.com

Продукты и аудитория

Комплексная платформа для управления привилегированными пользователями.

- Хранение и управление паролями, обнаружение учетных записей, SSH ключей, SSL сертификатов
- Контроль подрядчиков и администраторов по протоколам RDP\SSH\HTTP(s)\X11\VNC и тд
- Поведенческий анализ
- Управление привилегиями пользователей и запускаемыми приложениями
- Управление секретами DevSecOps

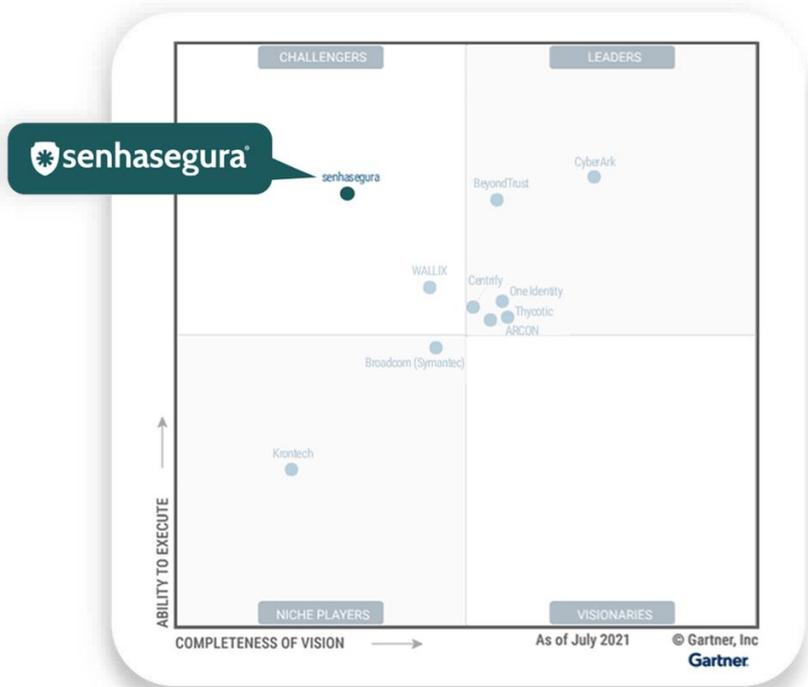


Согласно опросу Gartner за 2021 год:

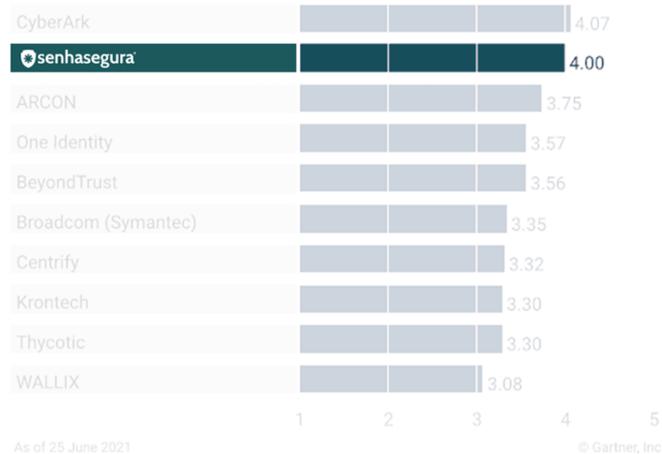
«Некоторые небольшие производители теперь предлагают более эффективные и менее дорогие решения, чем крупные и известные поставщики PAM».

Gartner
CHALLENGER

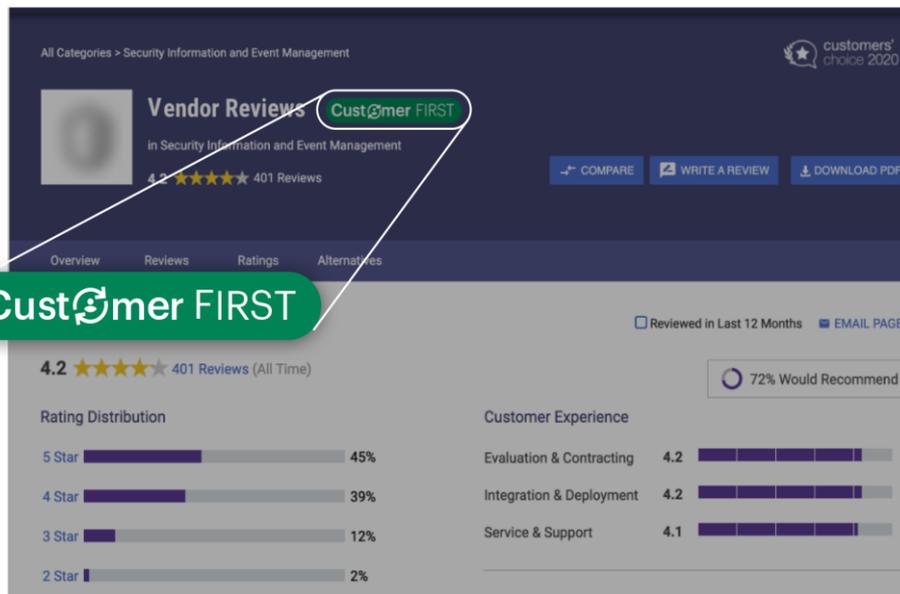
МАГИЧЕСКИЙ КВАДРАНТ GARTNER 2021



Оценка функций PAM-решений для средних и больших компаний



Отметки об участии в «CUSTOMER FIRST» и «CUSTOMER CHOICE» 2021



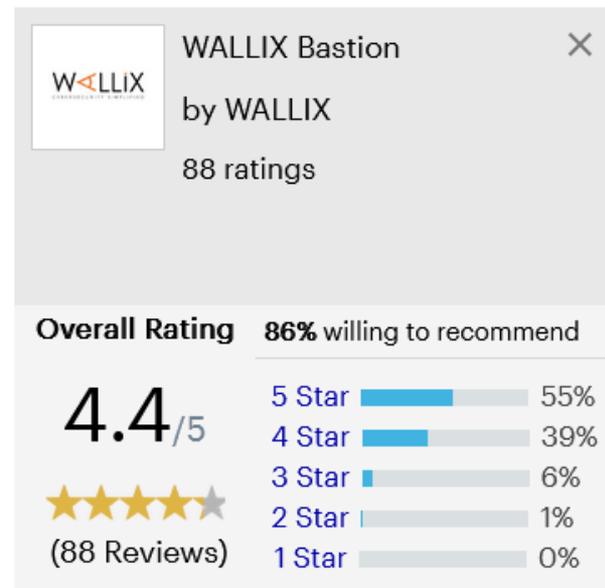
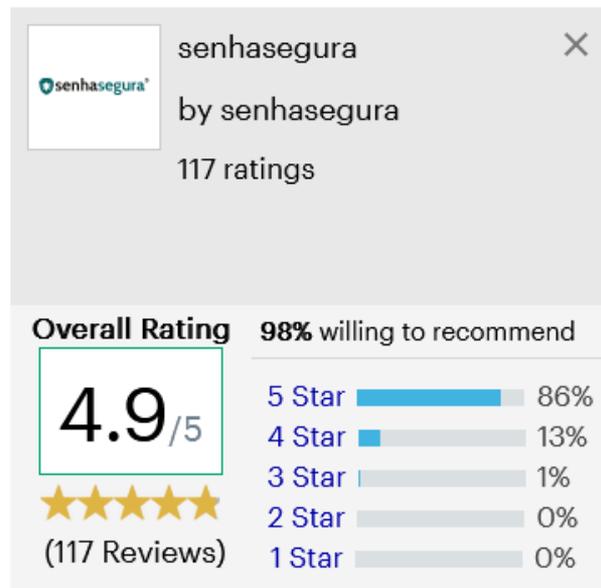
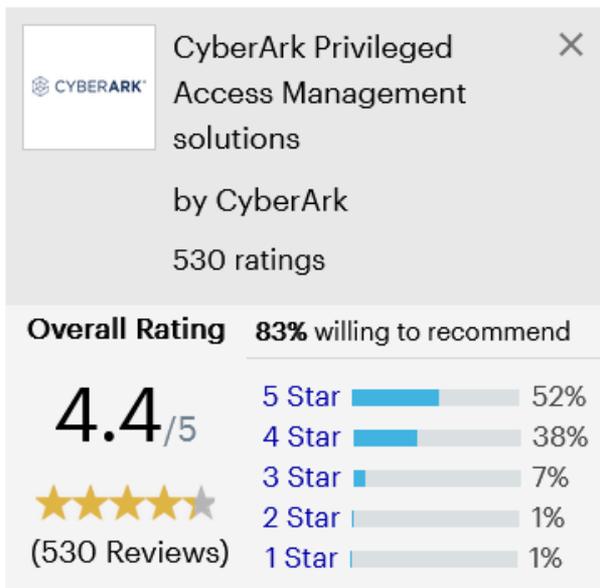
Senhasegura HE стремится заработать на своих услугах.

Мы хотим сделать их КАК МОЖНО ДОСТУПНЕЕ.



[GARTNER] «PEER INSIGHTS»

Senhasegura – лучшее решение по мнению пользователей Gartner Peer Insights в 2022 году и 98% рекомендовали бы это решение коллегам.



Злоупотребление привилегиями сегодня

Раньше организациям был необходим контроль только за доступом людей.

С приходом облачных технологий потребность в компьютерной автоматизации стала реальностью. **Управлять привилегированным доступом только сотрудников внутри компании уже недостаточно.**

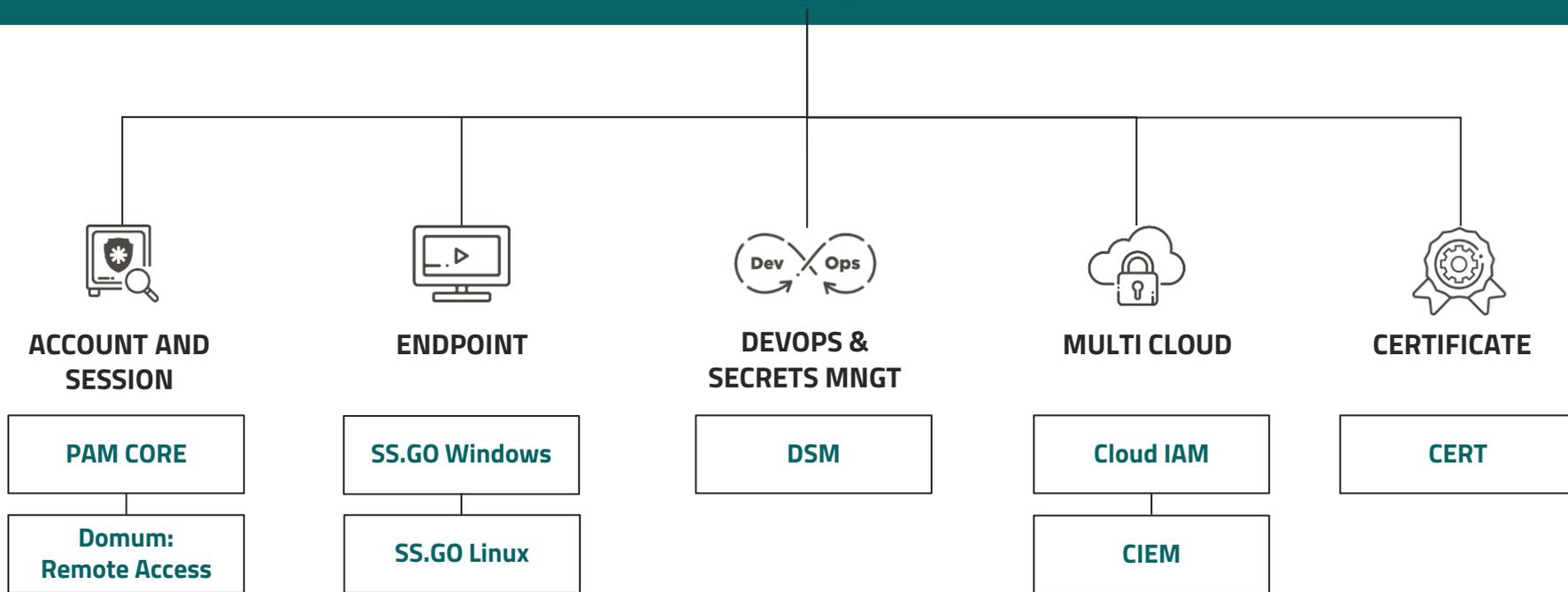
Сложность и масштабность управления доступом представляют **большую угрозу для суверенитета данных организации.**

В сочетании с разнообразием IoT и DevOps устройств они сделали злоупотребление привилегиями серьезной проблемой. **Пришло время управлять привилегированным доступом для машин и приложений как внутри организации, так и за ее пределами.**

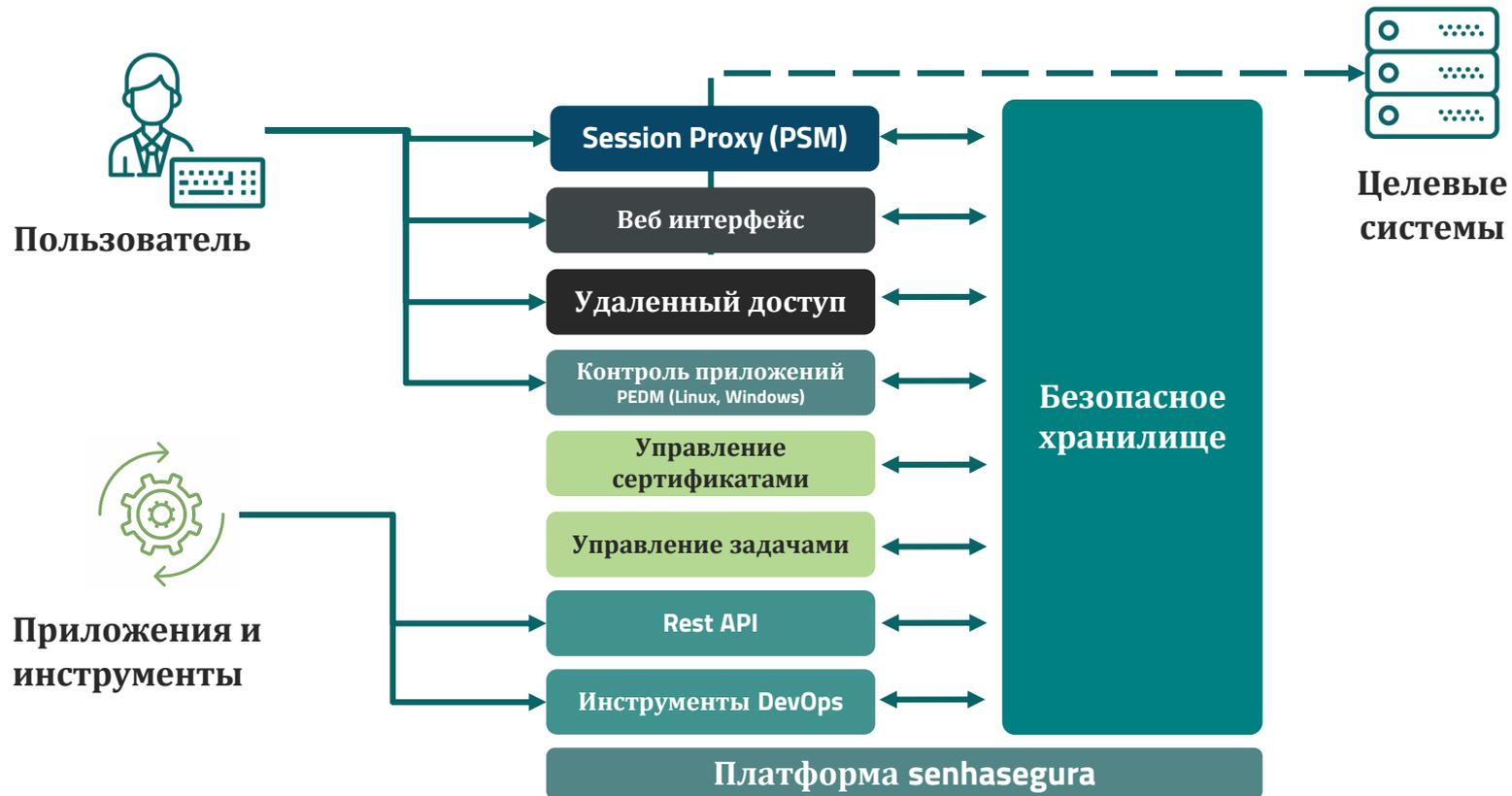
Понимание ситуации на рынке

Проблема	Последствия	Решение Senhasegura
<ul style="list-style-type: none">• РАМ сложен, и платформами часто тяжело управлять.	<ul style="list-style-type: none">• Сложность приводит к недоиспользованию инвестиций в РАМ.• Ложное восприятие безопасности и приуменьшение рисков.• Планы по развертыванию расширенных возможностей РАМ часто откладываются или отменяются.	<ul style="list-style-type: none">• Интуитивно понятный пользовательский интерфейс и легкость развертывания — простая навигация, развертывание занимает 7 минут, отличная поддержка и обучение, если вам потребуется дополнительная помощь.• 100% успех — мы работаем с нашими клиентами, чтобы обеспечить успешное развертывание и интеграцию в пользовательские среды.

Платформа



Платформа Senhasegura «все в одном»



АРХИТЕКТУРА SENHASEGURA

Другие решения

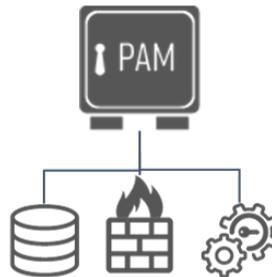
До 1000 устройств, 1000 соединений



Дорогое решение!

Преимущество senhasegura

До 1000 устройств, 1000 соединений



1 Linux сервер

- Встроенная База данных
- Встроенный межсетевой экран

Решение

Единое OVA-решение со всеми необходимыми лицензиями!*

*для обеспечения высокой доступности понадобятся дополнительные лицензии

Пример, системные требования для **500** одновременных сессий доступа RDP\SSH\HTTP:
Один сервер с **36** ядрами CPU, **32** Гб RAM

Обнаружение учетных записей

Senhasegura сканирует среду и обеспечивает автоматическую регистрацию устройств и их соответствующих учетных данных в решении.



Проблема

Большой объем учетных записей и устройств в сети создает проблемы при управлении и создает риски утечек и атак.

Решение

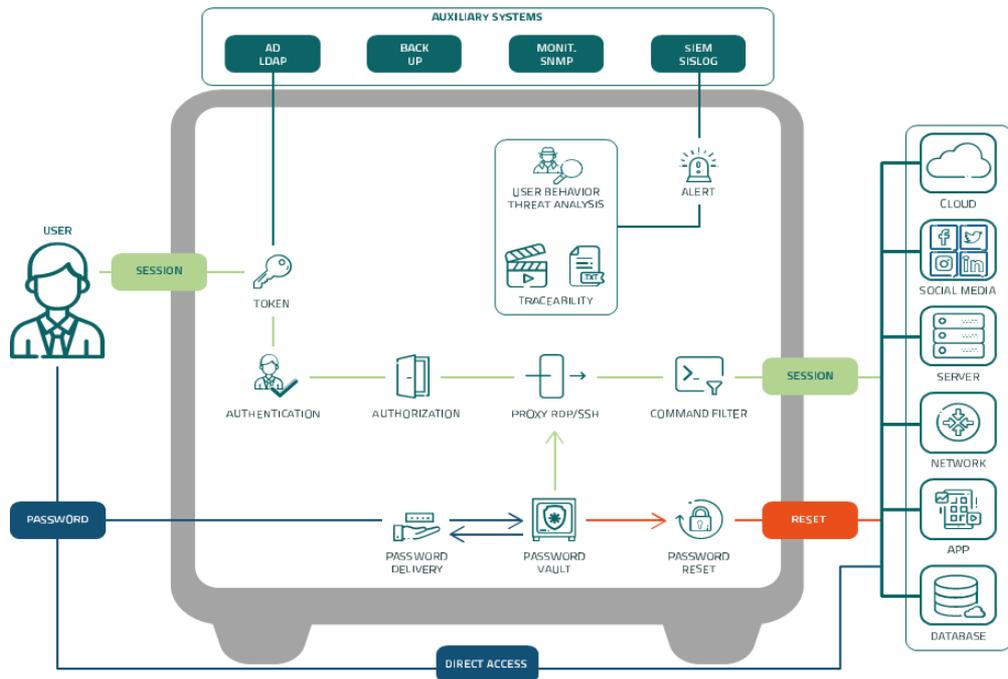
Полное сканирование среды с импортом всех учетных данных в безопасное хранилище.

Результат

Снижайте риск атак за счет устранения неуправляемых учетных записей.

PAM Core

Senhasegura может защитить привилегированные учетные записи и предотвратить злоупотребления привилегиями.



Проблема

Отсутствие контроля над привилегированными учетными данными мешает обеспечению безопасности и не защищает от злоумышленников.

Решение

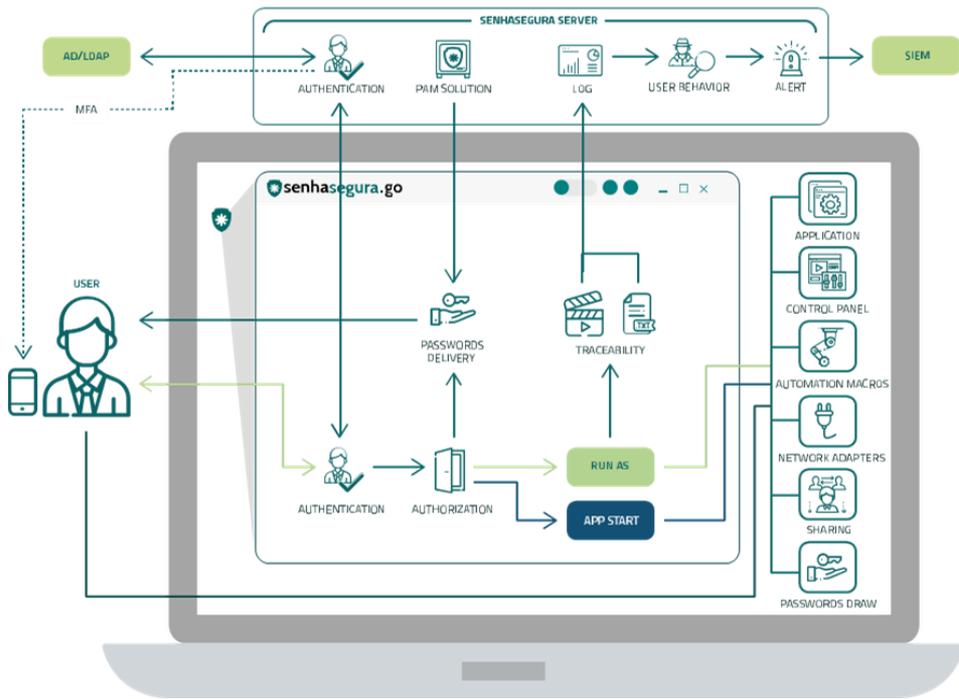
Обнаружьте и централизуйте все привилегированные учетные данные и создайте надежную аутентификацию, авторизацию и подотчетность для их использования.

Результат

Уменьшайте риски атаки, удалив ненужные учетные данные.

GO Endpoint Manager (PEDM) для Windows и Linux

Senhasegura может предотвратить злоупотребление привилегиями на Linux и Windows, надежно контролируя использование привилегированных учетных данных.



Проблема

Отсутствие контроля над привилегированными учетными данными на рабочих станциях не позволяет обеспечить высокий уровень безопасности, чем могут воспользоваться злоумышленники.

Решение

Модуль PEDM от **Senhasegura** безопасно управляет привилегированными учетными данными рабочей станции, контролирует использование и ведет подробный аудит действий.

Результат

Повышайте уровень безопасности рабочих станций.

Менеджер задач (входит в PAM)

Senhasegura может создавать и автоматизировать привилегированные задачи, чтобы исключить прямой сеанс привилегированного доступа к ресурсам инфраструктуры, уменьшая возможности атак.



Проблема

Операционные потребности требуют чрезмерно привилегированных сессий доступа к критическим ресурсам, что позволяет атаковать даже при отслеживании ответственности.

Решение

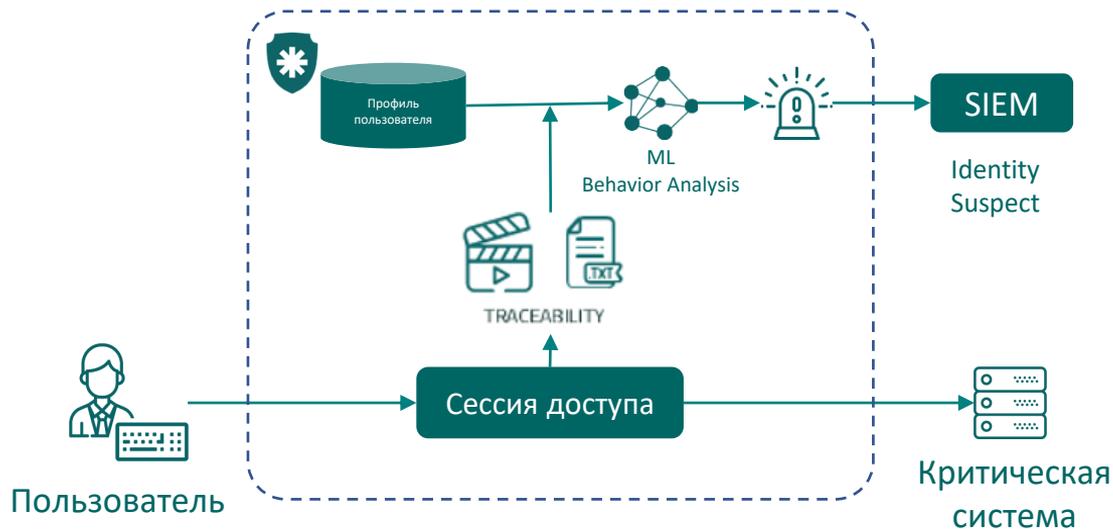
Senhasegura представила модуль для выполнения привилегированных задач на определенных устройствах без необходимости прямого доступа к критически важным устройствам.

Результат

Повышайте безопасность и производительность, снижайте операционные риски.

Поведенческий анализ пользователей

Senhasegura может отслеживать поведение пользователей в режиме реального времени, чтобы мгновенно определять подозрительное поведение и предотвращать злонамеренные действия.



Проблема

Хотя PAM-решения и обеспечивают подотчетность, злоумышленники все же могут получить доступ к учетным данным.

Решение

Senhasegura проводит мониторинг поведения пользователя в реальном времени, чтобы автоматически обнаруживать и останавливать злоупотребление привилегиями в случае необычного поведения.

Результат

Обнаруживайте злонамеренные действия в режиме реального времени, позволяя сократить время реакции.

Управление жизненным циклом сертификатов

Senhasegura может управлять всем жизненным циклом сертификата от его создания до публикации, чтобы повысить безопасность и эффективность.



Проблема

Контроль использования сертификатов, истечения срока их действия и требований безопасности.

Решение

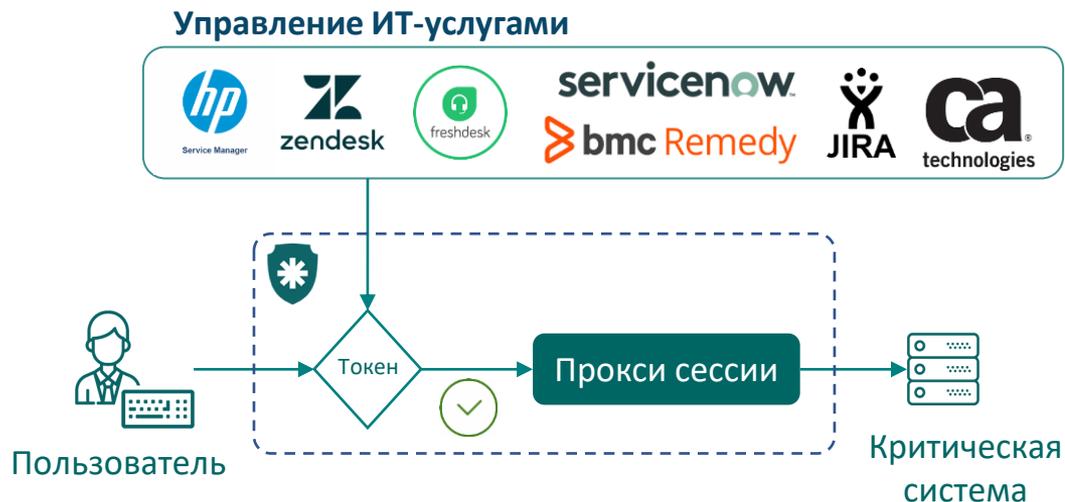
На протяжении всего процесса интеграции PAM Senhasegura управляет всем жизненным циклом сертификата, от обнаружения и истечения срока действия до автоматического обновления и повторной публикации.

Результат

Сокращайте простои бизнеса и доводите эффективность и безопасность до более высоких стандартов.

Интеграция с ITSM

Senhasegura может интегрироваться с основными ITSM-решениями, чтобы предотвращать несанкционированные изменения и улучшать управление.



Проблема

Изменения, несвязанные с процессом управления.

Решение

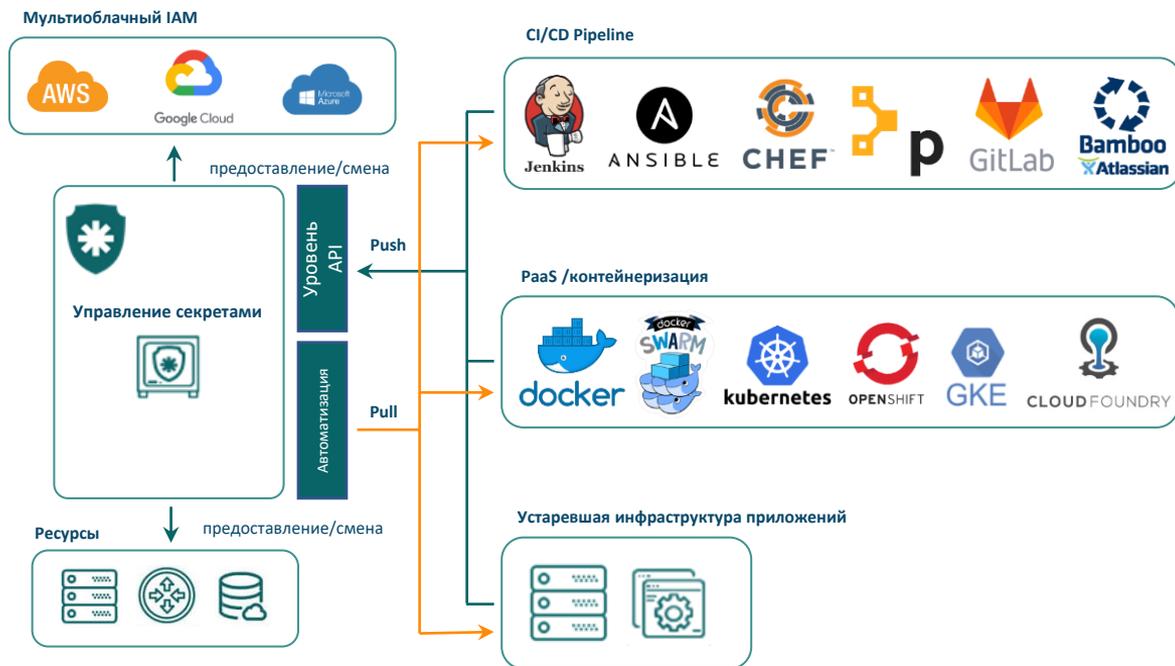
Senhasegura интегрируется с системами управления ИТ-услугами (ITSM), чтобы гарантировать выполнение только санкционированных изменений.

Результат

Снижайте риски простоев и операционные риски на уровнях управления.

DevSecOps: управление секретами

Senhasegura может управлять секретами в разнородных средах, чтобы гарантировать видимость, безопасность и доступ приложений.



Проблема

Внедрение практики DevOps создает многочисленные проблемы управления привилегиями в динамической, эластичной и крупномасштабной структуре, что приводит к снижению уровня безопасности.

Решение

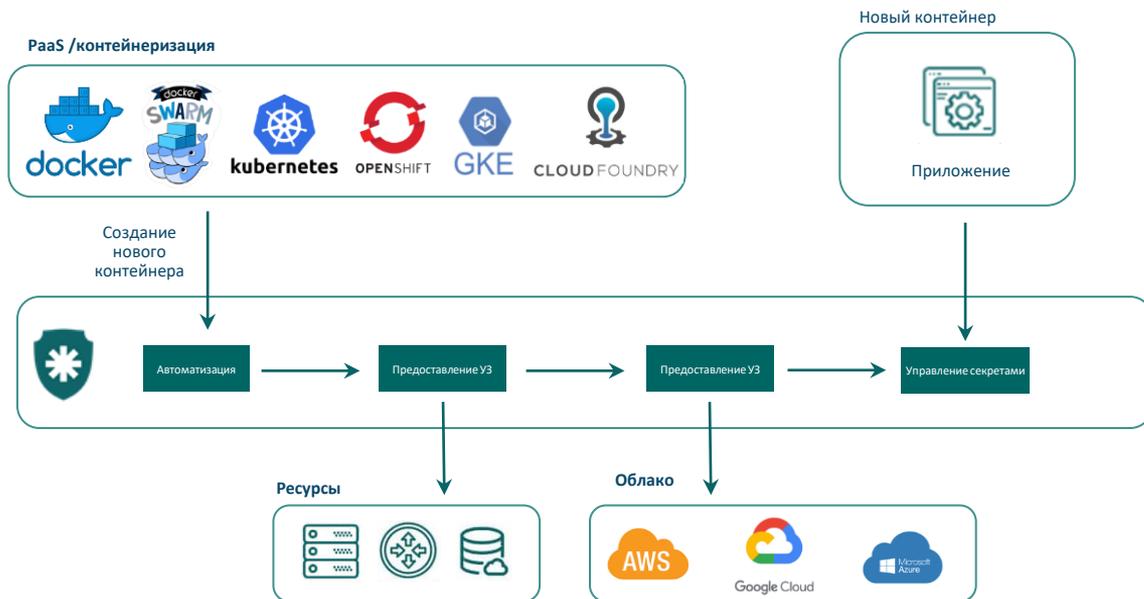
Модуль **Senhasegura** для автоматического обнаружения, управления, ротации и предоставления секретов помогает избежать жестко прописанных в коде ключей, учетных данных и сертификатов.

Результат

Достижайте высокого уровня безопасности в средах DevOps.

DevSecOps: предоставление доступа Just-In-Time

Senhasegura контролирует динамическое создание и удаление учетных записей в эластичной среде.



Проблема

Использование одного и того же набора учетных данных в контейнерах снижает уровень безопасности.

Решение

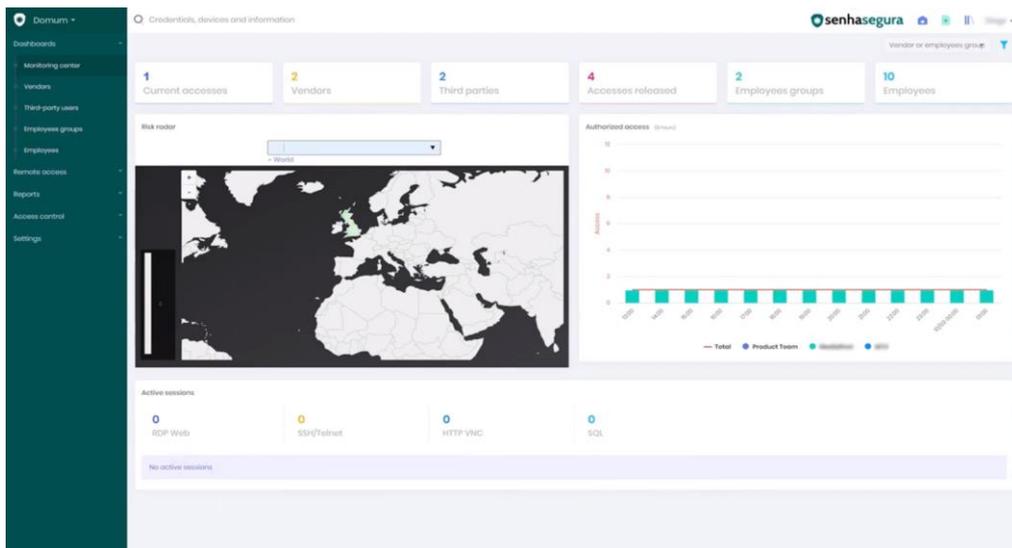
Индивидуальные секреты для каждого приложения и контейнера.

Результат

Безопасно работайте с учетными данными в контейнерах и приложениях.

DOMUM Remote Access

Senhasegura DOMUM Remote Access предлагает удаленный доступ для сотрудников и сторонних организаций на основе принципа нулевого доверия к сети компании без необходимости использования VPN.



Проблема

Необходимость иметь доступ с нулевым доверием для удаленных сотрудников и сторонних организаций без необходимости использования VPN.

Решение

Когда сотрудникам или сторонним организациям необходим доступ к устройствам, управляемым PAM-платформой, мы отправляем конечному пользователю ссылку для подтверждения доступа, что обеспечивает мгновенный и безопасный доступ к разрешенным устройствам.

Результат

Получайте операционную выгоду в управлении удаленными пользователями и максимальное разделение доступа на основе детализации.

МОДЕЛИ ЛИЦЕНЗИРОВАНИЯ

Все модули могут быть развернуты виртуально (публично или локально) или физически (оборудование)

- **PAM Core** – оплата за количество пользователей (неограниченное количество учетных данных и устройств и один бесплатный узел высокой доступности) – **Бессрочная лицензия, подписка и SaaS**
- **Certificate Manager** – оплата за количество сертификатов для оповещений об обнаружении – **Подписка и SaaS**
- **DevOps Secret Management** – по количеству приложений и секретов – **Бессрочная лицензия, подписка и SaaS**
- **GO Endpoint Manager(PEDM)** – оплата за количество устройств – **Бессрочная лицензия и подписка**
- **DOMUM Remote Access** – оплата за количество пользователей – **SaaS**

ОСТАЛИСЬ ВОПРОСЫ?

Попцов Сергей,
технический директор AFI Distribution
www.afi-d.ru | sp@afi-d.ru
Мобильный: +7 926 499-99-36
(+whatsapp/telegram)