AFI Distribution

www.AFI-Distribution.ru

PAM

# senhasegura®

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

2021

# Проект Senhasegura

Аудитория и решения

## 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

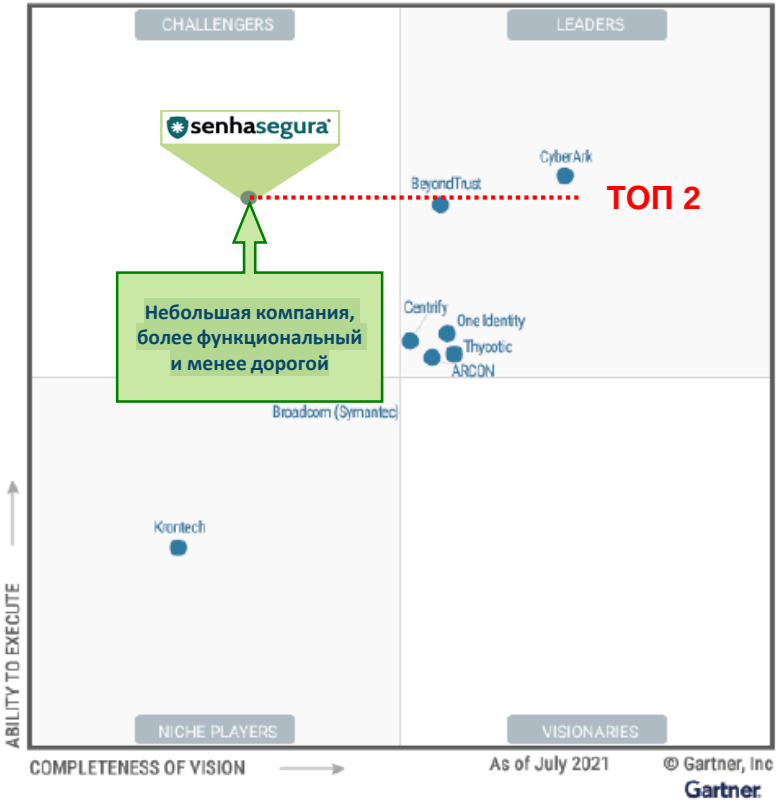
senhasegura®

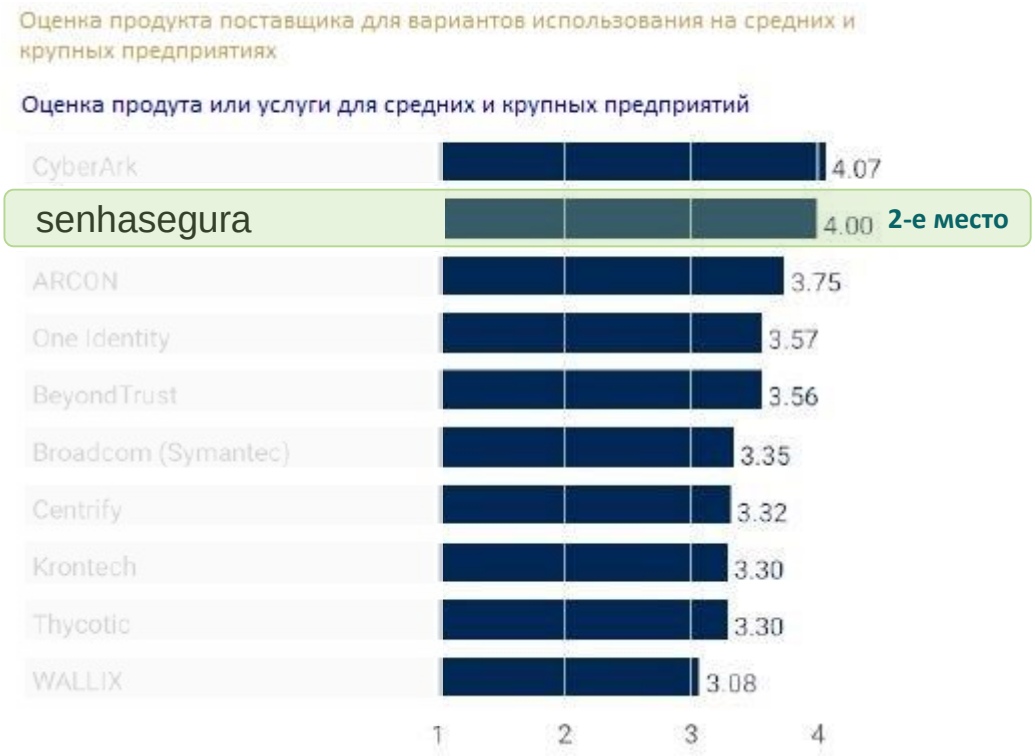
**Согласно опросу Gartner за 2021 год:**

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

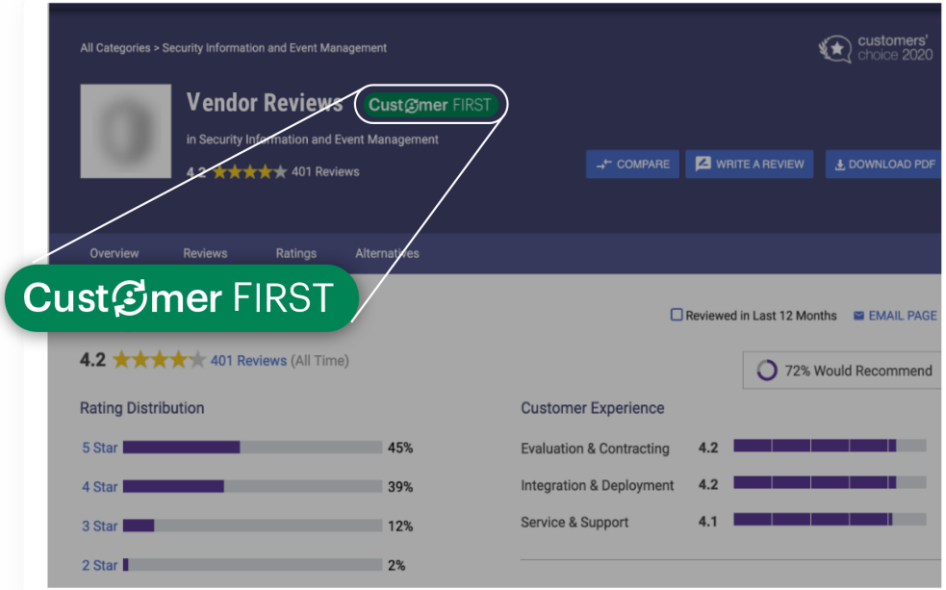
Gartner CHALLENGER

# МАГИЧЕСКИЙ КВАДРАНТ GARTNER 2021



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




**Senhasegura НЕ стремится заработать на своих услугах.**

**Мы хотим сделать их КАК МОЖНО ДОСТУПНЕЕ.**

Gartner peerinsights Customer FIRST

Gartner peerinsights customers' choice 2021 ™

# [GARTNER] «PEER INSIGHTS»

https://www.gartner.com/reviews/market/privileged-access-management/compare/product/beyondtrust-privileged-remote-access-vs-cyberark-privileged-access-management-solutions-vs-senhasegura-vs-thycotic-secret-server

| BeyondTrust Privileged Remote ... by BeyondTrust | CyberArk Privileged Access Man... by CyberArk | senhasegura by senhasegura | Thycotic Secret Server by Thycotic |
|---|---|---|---|
| 4.7 ★★★★★ | 4.48 ★★★★½ | 4.79 ★★★★★ | 4.61 ★★★★½ |
| 5 Star 67% | 5 Star 54% | 5 Star 81% | 5 Star 64% |
| 4 Star 29% | 4 Star 37% | 4 Star 18% | 4 Star 30% |
| 3 Star 4% | 3 Star 7% | 3 Star 1% | 3 Star 5% |
| 2 Star 0% | 2 Star 1% | 2 Star 0% | 2 Star 1% |
| 1 Star 0% | 1 Star 1% | 1 Star 0% | 1 Star 0% |
| 92% Yes | 83% Yes | 98% Yes | 86% Yes |

# 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**.

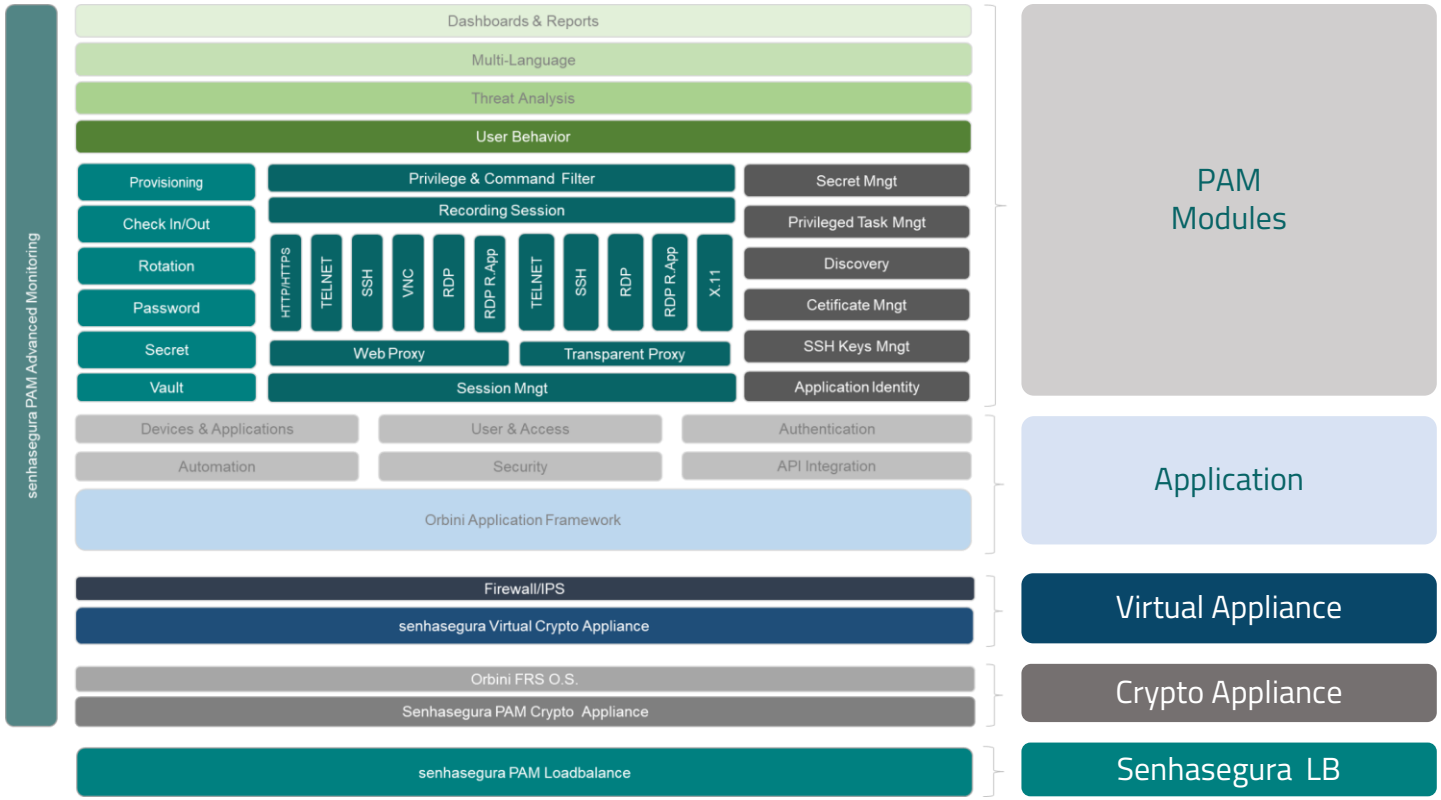
Gartner
CHALLENGER

# Понимание ситуации на рынке

| Проблема | Последствия | Решение Senhasegura |
|---|---|---|
| • **PAM сложен,** и платформами часто тяжело управлять. | • Сложность приводит к **недоиспользованию инвестиций в PAM**.<br><br>• **Ложное восприятие безопасности и приуменьшение рисков**.<br><br>• Планы по **развертыванию** расширенных возможностей PAM часто **откладываются** или отменяются. | • **Интуитивно понятный пользовательский интерфейс и легкость развертывания** — простая навигация, развертывание занимает 7 минут, отличная поддержка и обучение, если вам потребуется дополнительная помощь.<br><br>• **100% успех** — мы работаем с нашими клиентами, чтобы обеспечить успешное развертывание и интеграцию в пользовательские среды. |

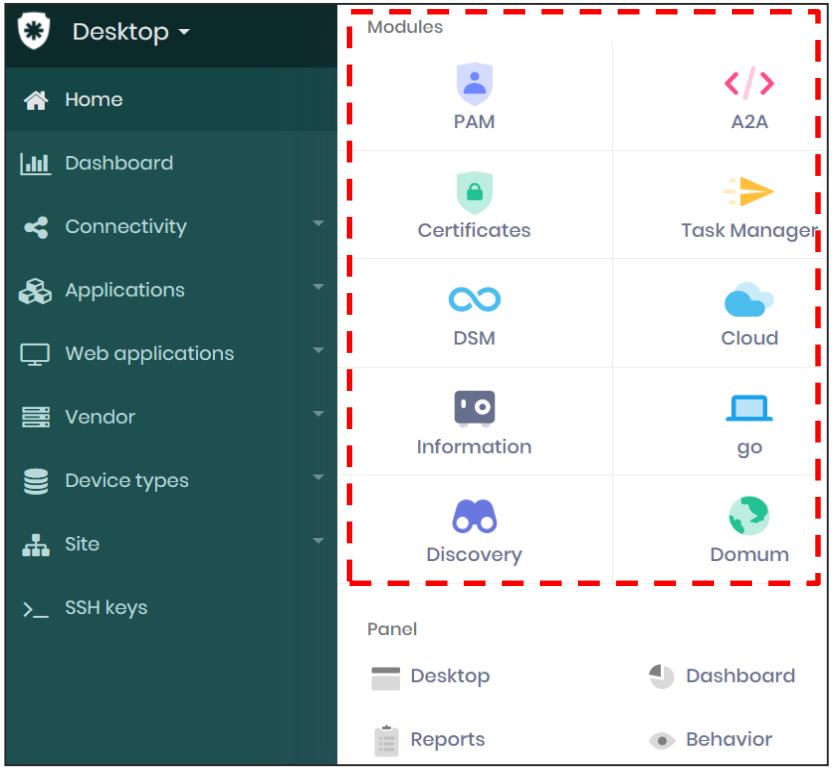
Gartner
CHALLENGER

# Архитектура




Gartner
CHALLENGER

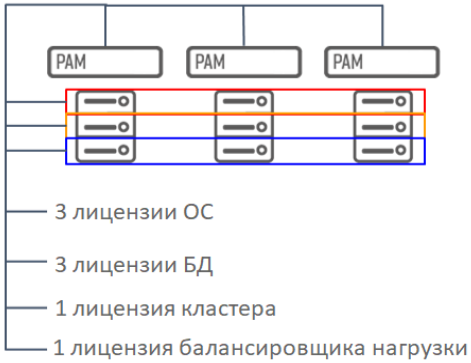
# УНИКАЛЬНОЕ ИНТЕГРИРОВАННОЕ РЕШЕНИЕ «ВСЕ В ОДНОМ»



# АРХИТЕКТУРА SENHASEGURA

## Другие решения

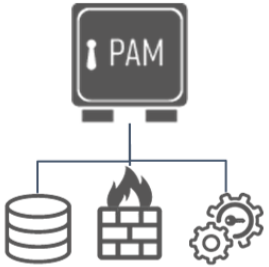
До 1000 устройств, 1000 соединений




**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**

Такой подход уменьшает количество необходимых серверов. Например, тот же проект для TIM* требовал только 6 серверов, когда они решили работать с senhasegura, в то время как в то время, если бы они перешли на CyberArk, тот же проект стоил бы им 64 дополнительных сервера, что более чем в десять раз больше, чем с senhasegura. *Клиент подпадает по соглашение о конфиденциальности.

# Обнаружение учетных записей

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

Обнаружение устройств

Обнаружение учетных записей на серверах, сетевом оборудовании и базах данных

Обнаружение SSH ключей

Обнаружение зависимых служб и пулов приложений

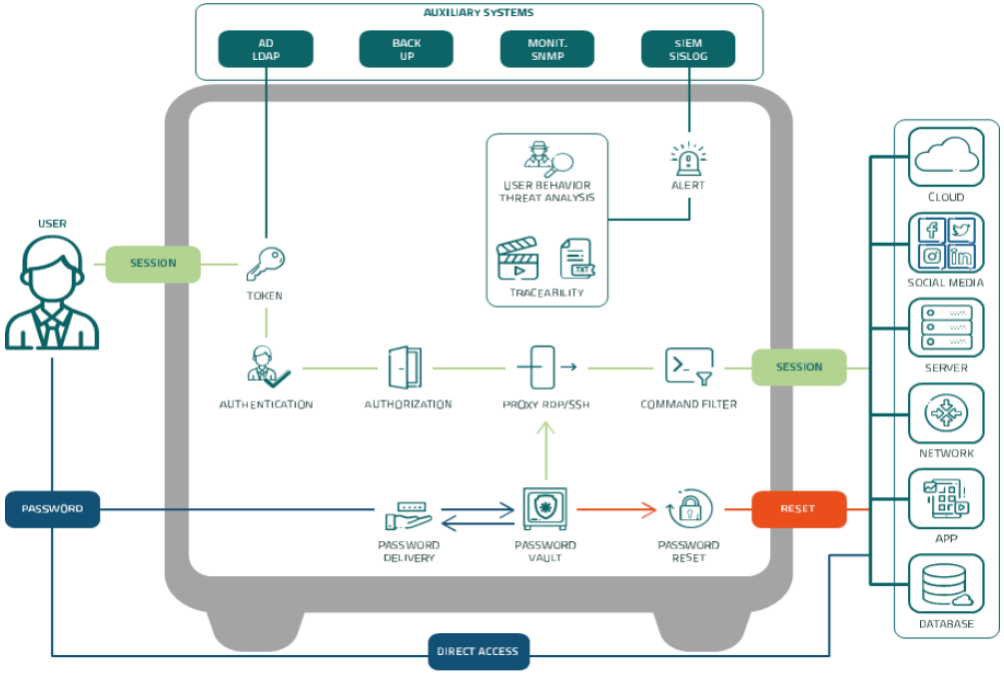
Обнаружение SSL сертификатов

Обнаружение контейнеров и DevOps артефактов

Gartner
CHALLENGER

# PAM PASM

**Senhasegura** может защитить привилегированные учетные записи и предотвратить злоупотребления привилегиями.




Хранение и управление паролями, ротация паролей и ключей SSH

Контролируемый доступ к целевым системам по RDP\SSH\HTTP(s)\X11\VNC и другим протоколам

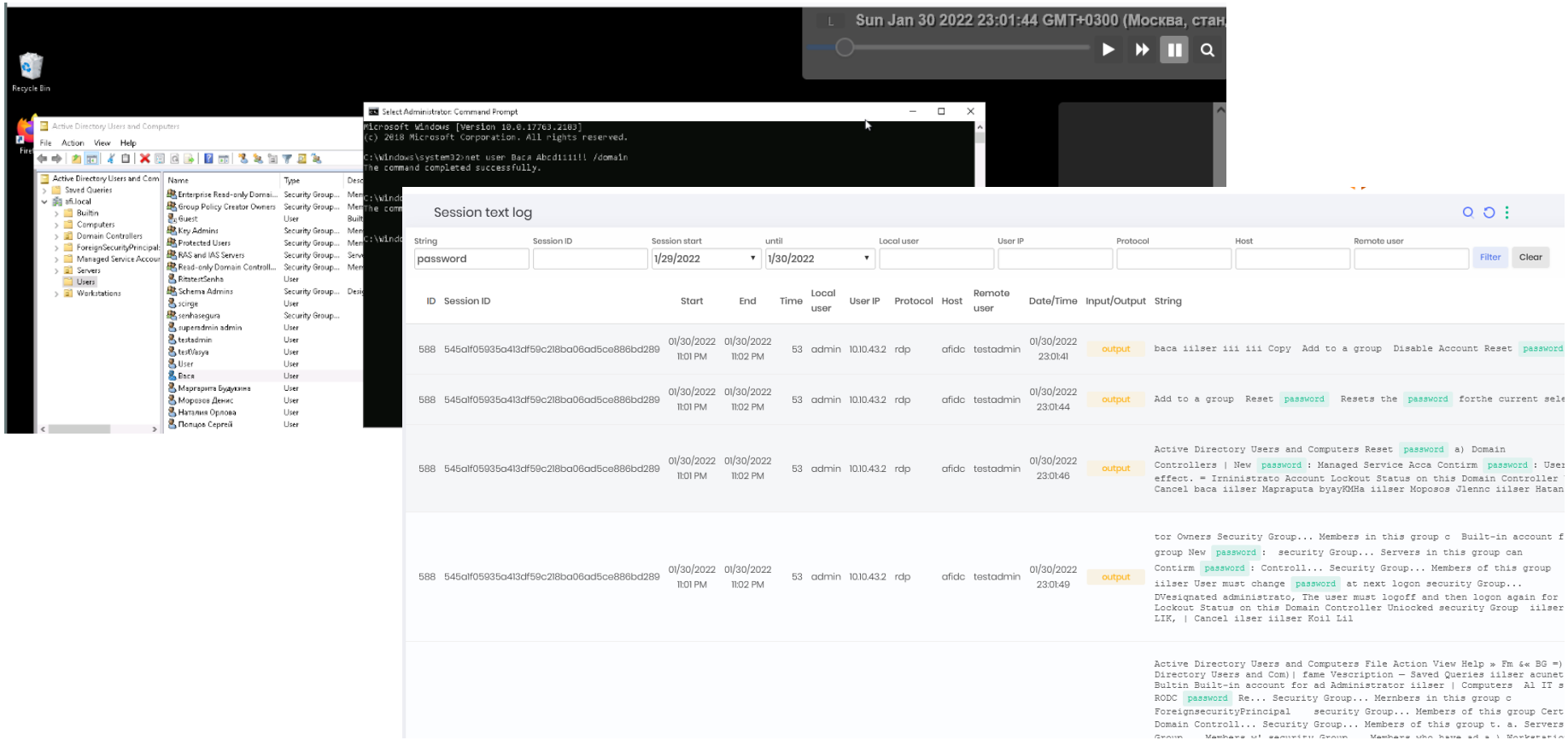
Запись сессий и поведенческий анализ действий пользователей

Менеджер задач и средства автоматизации

Ограничение выполняемых команд

Gartner CHALLENGER

# Скриншот: запись видео и распознавание текста в сессии



# Скриншот: переданные файлы и введенные команды

## Session logs

Search term

Search

*0 occurrences*

```
1643573898009 | Sun, 30 Jan 2022 23:18:18 +0300 |   system data | <Control_L><Shift_L>ls<
1643573898009 | Sun, 30 Jan 2022 23:18:18 +0300 | friendly data | ls
1643573905710 | Sun, 30 Jan 2022 23:18:25 +0300 |   system data | sudo apt-0get <BackSpac
ce><BackSpace><BackSpace><BackSpace>get update<Return>
1643573905710 | Sun, 30 Jan 2022 23:18:25 +0300 | friendly data | sudo apt-get update
1643573917314 | Sun, 30 Jan 2022 23:18:37 +0300 |   system data | top<Return>
1643573917314 | Sun, 30 Jan 2022 23:18:37 +0300 | friendly data | top
1643573921861 | Sun, 30 Jan 2022 23:18:41 +0300 |   system data | <Control_L>ccd ./<Retur
1643573921861 | Sun, 30 Jan 2022 23:18:41 +0300 | friendly data | cd ./
1643573929042 | Sun, 30 Jan 2022 23:18:49 +0300 |   system data | ls<BackSpace><BackSpace
<Return>
1643573929042 | Sun, 30 Jan 2022 23:18:49 +0300 | friendly data | datetime
1643573932416 | Sun, 30 Jan 2022 23:18:52 +0300 |   system data | exit<Return>
1643573932416 | Sun, 30 Jan 2022 23:18:52 +0300 | friendly data | exit
```

## Audited commands

| ID | Name | Command | Criticality | Type | Enabled |
|---|---|---|---|---|---|
| | | | All | All | Yes |

| ID | Name | Command | Criticality | Type | Action during session |
|---|---|---|---|---|---|
| 1 | Control Password Change - Linux | /.*passwd.*/ | Medium | Credential | Allow |
| 2 | Audit LS | ls | Low | Global | Allow |
| 3 | LS for group | /.+ls.+$/ | Medium | Group | Allow |
| 5 | Reboot command | /.+reboot.+$/)* | High | Global | Allow |
| 6 | su root | su root | High | Global | Lock |

Total: 5 records

## Transferred files

| File | MIME Type | SHA256 Checksum | Include | until |
|---|---|---|---|---|
| | | | 1/30/2021 | 1/30/2022 |

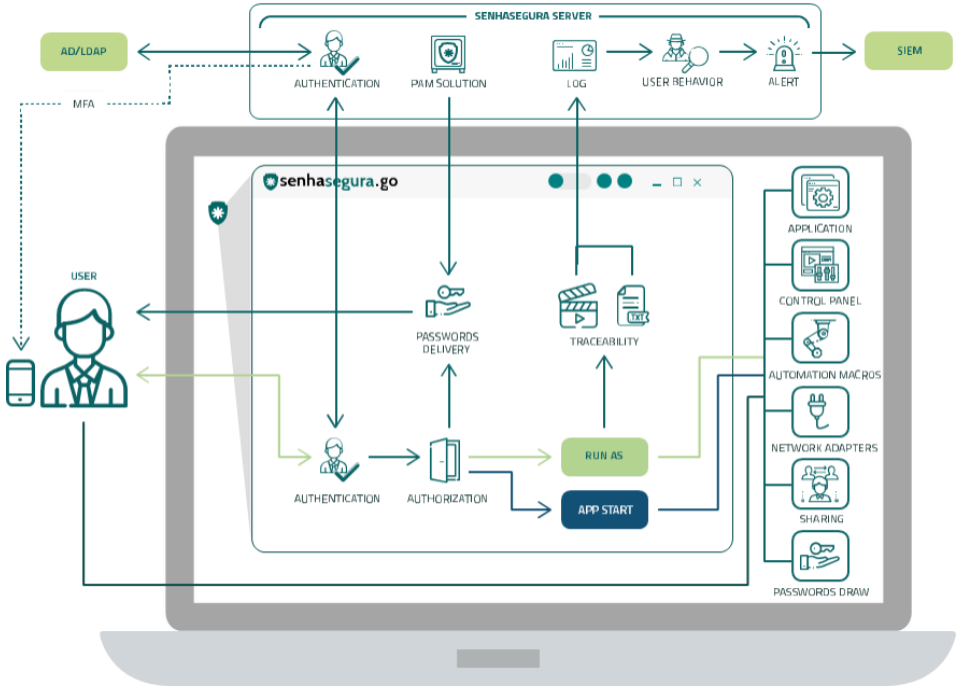
| Host | Port | Remote user |
|---|---|---|
| | | |

Filter Clear

| ID | File | Size Bytes | MIME Type | Include | User code | User IP | User | Host | Port | Remote user | SHA256 Checksum |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1.pdf | 1,312,332 | application/pdf | 08/17/2021 9:11 AM | 7 | 10.10.43.2 | Admin | 10.10.43.2 | 22 | afi | 84d40807025acabdb39af86e5543b4b42f0e13085e5c57ce6952199e3fe1f9e3 |
| 2 | New Text Document.txt | 15 | text/plain | 09/14/2021 12:38 PM | 96 | 10.10.43.2 | Попцов Сергей | 10.10.53.10 | 3389 | testadmin | 5d2744dabc7b25199142a15da209f87fef968f0c21796227e65f468f49b88115 |
| 3 | \Costa Rican Frog.jpg | 354,633 | image/jpeg | 09/14/2021 12:40 PM | 96 | 10.10.43.2 | Попцов Сергей | 10.10.53.1 | 3389 | testadmin | 92e6e0134e95e9555e1a324b39cd8e35af51457f8f52f104bfee09c3db565b6a |
| 4 | \afilogo-sq-1200.png | 30,687 | image/png | 09/14/2021 1:08 PM | 96 | 10.10.43.2 | Попцов Сергей | 10.10.53.50 | 3389 | user | 66288338f97eca5640dc27a05a406e1ba92a8449af08bbbd00b6833d530ed9c2 |

# PAM PEDM для Windows и Linux

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




Контроль привилегий и запускаемых приложений

Аудит запускаемых приложений и команд

Ограничение команд CMD и PowerShell

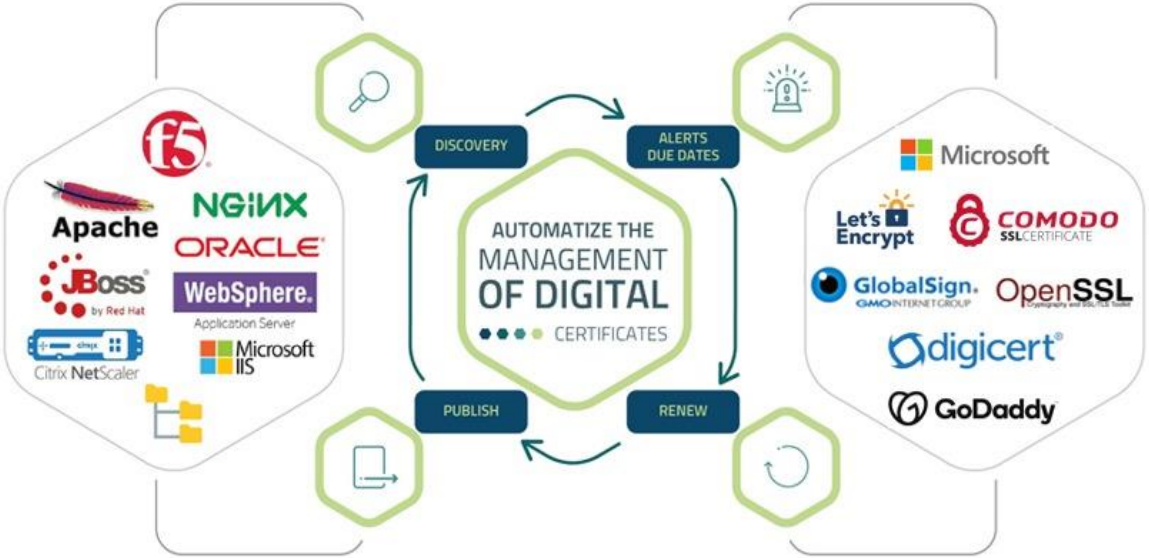
Временное получение прав локального администратора с видеозаписью действий

Поведенческий анализ действий пользователей

Gartner CHALLENGER

# Управление жизненным циклом сертификатов

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




Управление сертификатами SSL

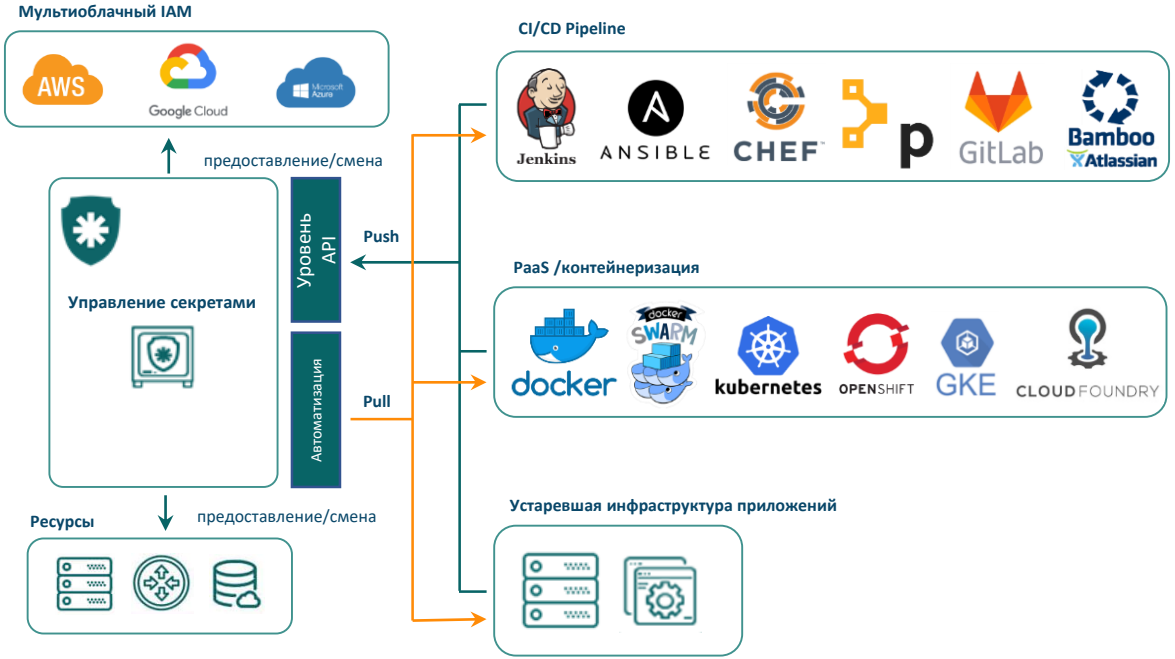
Автоматическая ротация SSL сертификатов

Контроль сроков действия сертификатов

Gartner CHALLENGER

# DevSecOps: управление секретами

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




Безопасный обмен секретами между приложениями в DevOps процессах

Динамическое создание учетных записей

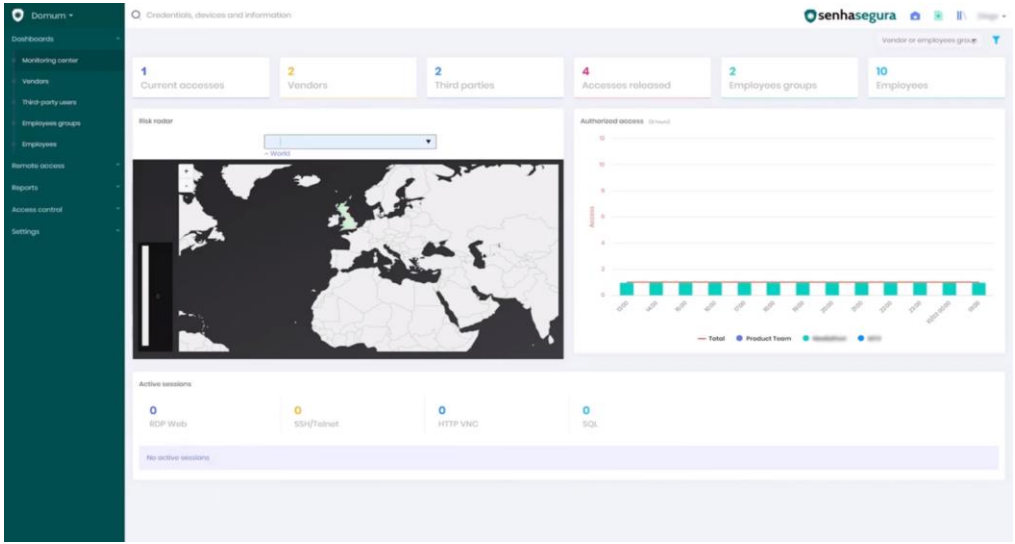
Индивидуальные учетные данные для каждого приложения и контейнера

Удаление ключей, токенов и других учетных данных из исходных кодов приложений

Gartner
CHALLENGER

# Инновация: Senhasegura DOMUM

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




Облачный сервис Senhasegura

Контролируемый удаленный доступ для ваших подрядчиков без использования VPN

Ежемесячная подписка, позволяющая предоставлять временный доступ подрядчикам без расширения лицензии на PAM.

Gartner
CHALLENGER

# МОДЕЛИ ЛИЦЕНЗИРОВАНИЯ

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

- **PAM** – оплата за количество пользователей (неограниченное количество учетных данных и устройств и один бесплатный узел высокой доступности) – **Бессрочная лицензия, подписка и SaaS**
- **CI Management and Renew** – оплата за количество сертификатов для оповещений об обнаружении – **Подписка и SaaS**
- **DevSecOps** – оплата за количество приложений и секретов – **Бессрочная лицензия, подписка и SaaS**
- **PEDM – SSGO** – оплата за количество устройств – **Бессрочная лицензия и подписка**
- **DOMUM** – 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)