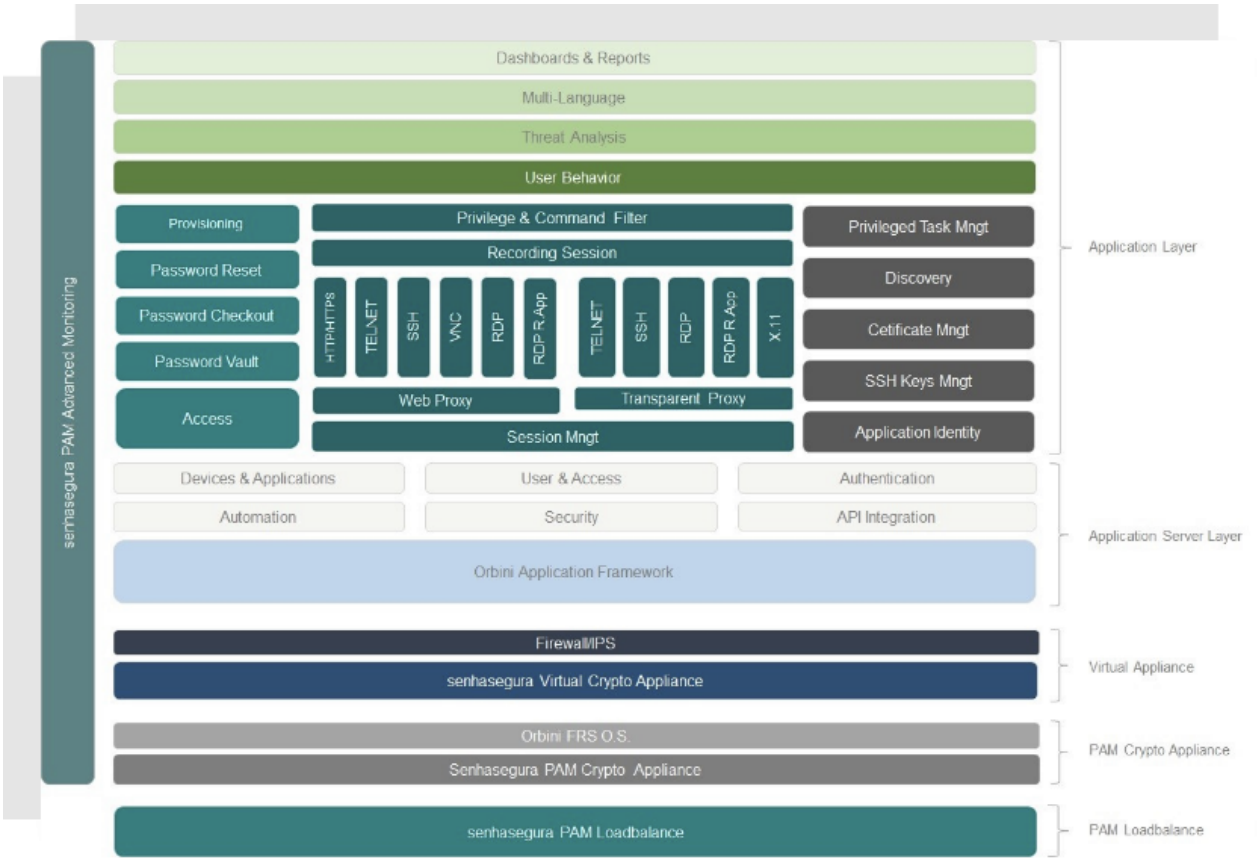
Техническая спецификация

Senhasegura — платформа по обеспечению информационной безопасности, состоящая из программного обеспечения, операционной системы и оборудования. Данная модульная платформа соответствует самым строгим стандартам безопасности в отрасли.

В этом документе мы рассмотрим основные технические аспекты Senhasegura.

Архитектура системных модулей

Программное решение Senhasegura разделено на следующие модули:



Эти компоненты поддерживают работу Senhasegura от физического уровня до уровня приложения.

- Business layer: здесь расположены все функции Senhasegura, от интеграции до записи активности.
- Application Server layer: здесь находится Orbit, MT4 разработала платформу для поддержки всех функций решения.

- Virtual Appliance: виртуальное устройство, на котором выполняется решение.
- Appliance layer: аппаратное решение Senhasegura.

Компоненты решения

В дополнение к представленным модулям решение имеет важные встроенные программные компоненты, интегрированные в него без необходимости использования внешних ресурсов:

1. Оптимизированная и усиленная по всем аспектам (приложение, база данных, файловая система и т. д.) операционная система на базе Linux. В системе запущено только минимальное количество служб, соответствующих принципу минимальных привилегий, и ядро, адаптированное к функциональности решения.
2. Собственная база данных; без необходимости докупать лицензию.
3. Собственный интегрированный веб-сервер.
4. Встроенный веб-интерфейс, без необходимости приобретения дополнительных лицензий или функций для использования. Имея всего один интерфейс настройки сети, у вас уже есть возможность получить доступ к HTTPS веб-интерфейсу, чтобы все остальные настройки можно было выполнять в безопасной и удобной графической среде.

Порты

Протокол/Порт	Функция
TCP/22	Сервер SSH
TCP/80	Веб-сервер с перенаправлением на порт 443
TCP/443	Сервер веб-приложений
UDP/161	SNMP
UDP/162	SNMP
TCP/3389	RDP прокси
TCP/3306	Кластер базы данных
TCP/4444	Кластер базы данных
TCP/4567	Кластер базы данных
TCP/4568	Кластер базы данных
UDP/4567	Кластер базы данных

Языки

Интерфейс решения доступен на следующих языках:

1. Бразильский португальский (PT-BR)
2. Американский английский (EN-US)
3. Немецкий (DE)
4. Испанский (ES)
5. Польский (PL)
6. Французский (FR)
7. Русский (RU)

Решение позволяет пользователю вводить и хранить данные с использованием кодировки UTF-8:

1. Арабский
2. Арабский расширенный-A
3. Арабский расширенный -B
4. Арабские математические алфавитные символы
5. Формы представления на арабском языке-A
6. Формы представления на арабском языке-B
7. Дополнение к арабскому языку
8. Базовая латиница
9. Расширенное бопомофо
10. Совместимость с CJK
11. Штрихи CJK
12. CJK символы и пунктуация
13. Унифицированные иероглифы CJK
14. Унифицированные иероглифы CJK
15. Расширение B унифицированных иероглифов CJK
16. Расширение C унифицированных иероглифов CJK
17. Расширение D унифицированных иероглифов CJK
18. Расширение E унифицированных иероглифов CJK
19. Расширение F унифицированных иероглифов CJK
20. Кириллица
21. Дополнение к кириллице
22. Приложенные письма CJK A
23. Французский
24. Совместимость с хангыль J
25. Иврит
26. Хирагана
27. Канбун
28. Катакана
29. Фонетические расширения катаканы
30. Расширенная латиница-A
31. Дополнение к латинице-1
32. Сирийский
33. Дополнение к сирийскому
34. Русский
35. Символ гексаграммы Ицзин

Поддерживаемые языки

Русский:
• Поддержка ввода и сохранения на целевом языке в веб-интерфейсе.
• Поддержка ввода и сохранения на целевом языке в интерфейсе RDP прокси-сервера.
• Поддержка ввода и сохранения на целевом языке в интерфейсе прокси Терминала.

- Поддержка индексации текста сессий (OCR).
- Раскладка клавиатуры.
- Перевод веб-интерфейса
- Перевод прокси-системы Терминала.
- Перевод системы веб-прокси.

Испанский:
- Поддержка ввода и сохранения на целевом языке в веб-интерфейсе.
- Поддержка ввода и сохранения на целевом языке в интерфейсе RDP прокси-сервера.
- Поддержка ввода и сохранения на целевом языке в интерфейсе прокси Терминала.
- Поддержка индексации текста сессий (OCR).
- Раскладка клавиатуры.
- Перевод веб-интерфейса.
- Перевод прокси-системы Терминала.
- Перевод системы веб-прокси.

Руководства пользователя

Решение предоставляет руководства пользователя на следующих языках:

1. Бразильский португальский (PT-BR)
2. Американский английский (EN-US)

ISO 27001, PCI, SOX, GDPR, PQO BM&F

Senhasegura позволяет организациям развертывать самые строгие и сложные средства управления привилегированным доступом к учетным данным, требуемые такими стандартами, как ISO 27001, PCI, SOX, GDPR и PQO. Это возможно благодаря автоматизации управления привилегированным доступом, защищая ИТ-парк от утечек данных и потенциальных нарушений соответствия.

Повышение безопасности

Повышение безопасности уменьшает вероятность атаки на систему за счет смены паролей по умолчанию, удаления ненужного программного обеспечения, удаления неиспользуемых пользователей или логинов, а также отключения или удаления ненужных служб.

Для снижения числа попыток атак Senhasegura использует ряд процессов защиты, признанных рынком безопасности, на разных уровнях приложения и его компонентов.

Среди других моделей Senhasegura использует процессы защиты, рекомендуемые NIST (Национальным институтом стандартов и технологий) и CIS (Центром безопасного интернета).

Процесс повышения безопасности пересматривается с каждым новым выпуском решения, чтобы он всегда соответствовал лучшим практикам и основным процессам безопасности, принятым на рынке.

Обновление компонентов

Группа исследований и разработки Senhasegura следит за обновлениями сторонних компонентов, из которых состоит решение. Обновление этих компонентов осуществляется через быстрый канал связи и проводится для клиентов, если появляется критический запрос.

Процесс обновления инструмента соответствует политике обновления клиента. В этом случае будет развернута команда для выполнения процесса установки с наименьшим риском влияния на бизнес заказчика.

Функциональные возможности по модулям

> ⚠ Senhasegura не позволяет устанавливать стороннее программное обеспечение.

Base Module – System access settings

Этот модуль имеет следующие функции:

• senhasegura Authentication: Senhasegura имеет свой модуль аутентификации с функциональностью, которая подразумевает блокировку пользователя после определенного количества неудачных попыток входа в систему. А также смену пароля при первом входе, проверку сложности нового созданного пароля со сравнением истории использованных паролей.
• User Registration: полная регистрация пользователей с отслеживанием изменений и конфигураций.
• Profile Management: расширенное детальное управление профилями с возможностью создания профиля для каждого пользователя.
• Screen's Log: журнал просмотра экрана системы.
• Screen Identification by codes: идентификация каждого системного экрана с помощью уникального кода, что делает доступными обслуживание и поддержку.
• External Authentication Servers: помимо модуля аутентификации, Senhasegura можно использовать в сочетании с другими службами каталогов. Вы можете настроить Senhasegura для выполнения аутентификации на нескольких серверах, включая установление порядка аутентификации. Центральными серверами аутентификации, которые интегрируются с Senhasegura, являются Active Directory, LDAP, TACACS и RADIUS.
• Two-Factor Authentication: вы можете усилить процесс аутентификации с помощью многофакторной аутентификации, например, используя приложение Google Authenticator.
• IP Access Blocking: Senhasegura может блокировать доступ через заранее созданный черный список IP-адресов.
• Session Management: в этом инструменте модуль управления сессиями отвечает за проверку достоверности сессии и установку времени ожидания до следующего входа в систему.
• Authentication with A1 and A3 Certificates: процесс аутентификации может осуществляться с использованием сертификатов A1 и A3 в качестве второго фактора аутентификации.

Base Module – Password and information vault

Этот модуль является основой хранилища паролей и выполняет следующие функции:

Password Guard: хранение паролей в хранилище, зашифрованном по алгоритму AES 256 с двойным коэффициентом шифрования. Доступ к паролям в этом модуле возможен только через модуль Access Management.
Protected Information Guard: хранилище паролей обеспечивает зашифрованное хранение информации, такой как токены, сертификаты и файлы.
Backup of Secrets: пароли, защищенная информация и ключи SSH требуют независимого модуля резервного копирования в решении.
Хранилище информации и пароли отвечают за запись секретов в резервную копию, зашифрованную с помощью главного ключа хранилища на основе алгоритма Шамира.

HSM Integration: интеграция с внешними или внутренними аппаратными модулями безопасности.

Base Module – Equipment register

Этот модуль представляет собой интерфейс паролей Senhasegura с оборудованием, пароли которого находятся под управлением. Модуль включает следующие функции:

- Registration Interface: регистрация оборудования. Индивидуально через веб-экран, либо в процессе регистрации всей партии оборудования.
- Connector Management: каждое устройство имеет порты для подключения и протокол доступа. Этот модуль управляет настроенными соединениями и взаимодействует с устройствами.
- Connectivity Test: Senhasegura периодически будет подключаться к зарегистрированным устройствам и проверять их подключение. Пользователи могут быть проинформированы о результатах данного тестирования.
- Equipment Profile: типы и модели оборудования имеют профили подкачки по умолчанию и шаблоны паролей в инструменте. Этот модуль связывает устройства с этими политиками.

Base Module – Access to information, passwords, and session policies

Модуль политики доступа является единственным, имеющим доступ к хранилищу паролей и информации. В нем представлены следующие функции:

Access Workflow: рабочий процесс доступа инициирует процесс согласования для доставки аутентифицированной сессии или пароля. Этот процесс имеет разные настройки и маршруты в зависимости от конфигурации клиента.
Access Approvation: функция подтверждения доступа позволяет утверждающему пользователю ответить на запрос доступа с помощью:
Экрана пользователя Электронной почты
SMS
Функции аварийного доступа

Password Split: эта функция отвечает за разделение пароля на две части для сегментированной доставки и соответствует требованиям стандарта PCI.
Access Control: модуль управления доступом объединяет три объекта, учитываемых

при принятии решения об отказе от учетных данных или доступа:
Delivery Policy Involved Users Related Equipment

Объединение этих объектов определяет критерии доставки сессий в системе.

User Timing: модуль контроля доступа может быть синхронизирован с сервером аутентификации. Пользователи определенной группы на сервере аутентификации загружаются в группы доступа Senhasegura, что упрощает управление доступом.

Base Module – Reports

◦ Reporting Configuration: пользователь может удалить или добавить информацию в тот или иной отчет через интерфейс. Вы можете создать совершенно новый способ визуализации полезной информации для ваших нужд.
◦ Shipping Schedule: созданные отчеты могут быть настроены на автоматическую отправку определенным пользователям.
◦ PCI Reports: набор специальных отчетов, отвечающих требованиям аудита стандарта PCI.
◦ Audit Trails: Senhasegura содержит отчеты со всеми соответствующими системными событиями. События можно экспортировать в SIEM и Syslog.

Base Module - Dashboards

System Health: функция отвечает за графическое отображение обзора оборудования и виртуальных машин Senhasegura. Здесь вы можете просматривать данные, такие как ввод-вывод, память и обработка.
Process Monitoring: отслеживает выполнение важных процессов хранилища:

Password Changes
Access Group Synchronisms Password Reconciliation Connectivity Tests
Settings Backup Password's backup

Business Monitoring: отслеживает работоспособность для защиты учетных данных и информации:

- Number of Passwords changed x Failures
- By period
- Number of Sessions:
- Active and Concurrent x System Average
- Recorded (by period)
- Average session time logged in
- Users logged in to the system

Password Change Module

SSH Password Change: устанавливает соединение и запускает сценарий обмена паролем по умолчанию на устройстве, используя протокол SSH, без необходимости установки агентов.
Windows Server: Windows Password Exchange подключается к серверу Windows и запускает локальные сценарии обмена паролями без установки агентов.
Используя собственные протоколы Microsoft (RPC, RM/WMI), Senhasegura может взаимодействовать с устройством с помощью команд из этих протоколов или через команды PowerShell, если включена его поддержка.

Network Asset: установка соединения и запуск сценария обмена паролем по умолчанию на устройстве по протоколу SSH без необходимости установки агентов.
Desktop: установка соединения и выполнение сценария обмена по умолчанию для этого пароля на этом рабочем столе, используя различные протоколы на рабочем столе.
Database: установка соединения и выполнение сценария обмена по умолчанию для этого пароля в этой базе данных, используя базовый протокол.

Password Reconciliation Module

Сверка паролей происходит одинаково на серверах, сетевых ресурсах, компьютерах и банках: периодически выполняется доступ к устройствам и учетным записям, пытаясь аутентифицироваться с использованием последнего сохраненного пароля, проверяя, остается ли хранение под безопасным паролем.

Management Module - Windows sessions

Session Delivery: доставка аутентифицированной сессии выполняется без ввода имени пользователя или пароля.
Session Recording: во время доступа к аутентифицированной сессии система выполняет ее запись в виде видео и текста.
MP4 Video Generation: записанное видео может быть сгенерировано в формате mp4 для скачивания и загрузки.
Audited Proxy Support: встроенная проверенная поддержка прокси-сервера для подключения клиентских приложений по SSH и RDP. Для совместимости между производителями все прокси-модули используют современные алгоритмы шифрования и собственные протоколы.

Management Module – Сессии Linux

Linux Web Session Delivery: доставка аутентифицированной сессии без ввода имени пользователя или пароля.
Web Session Recording: во время доступа к аутентифицированной сессии система выполняет ее запись в виде видео и текста.
MP4 Video Generation: записанное видео может быть сгенерировано в формате mp4 для скачивания и загрузки.
Audited Proxy Support: встроенная проверенная поддержка прокси-сервера для подключения клиентских приложений по SSH и RDP. Для совместимости между производителями все прокси-модули используют современные алгоритмы шифрования и собственные протоколы.

Management Module - SSH Gate Sessions - Senhasegura Terminal Proxy

◦ Linux Session Delivery via SSH Gate: доставка аутентифицированной сессии без ввода имени пользователя или пароля. Этот процесс прозрачен для пользователя через любой SSH-клиент.
◦ Web Session Recording: во время доступа к аутентифицированной сессии система выполняет ее запись в виде видео и текста.
◦ Command Audit: все команды, отправляемые на сервер через Senhasegura, проверяются и генерируются предупреждения о выполнении команд.
◦ Privilege Control: детальный контроль команд, которые могут быть выполнены с возможностью блокировки не авторизованных для пользователя команд.
◦ Audited Proxy Support: встроенная проверенная поддержка прокси-сервера для подключения клиентских приложений по SSH и RDP. Для совместимости между

производителями все прокси-модули используют современные алгоритмы шифрования и собственные протоколы.

Management Module - HTTP Sessions

• HTTP and HTTPS Session Delivery: доставка аутентифицированной сессии на страницу без необходимости ввода имени пользователя или пароля.
• Web Session Recording: во время доступа к аутентифицированной сессии система записывает видео.
• MP4 Video Generation: записанное видео может быть сгенерировано в формате mp4 для скачивания и загрузки.

Discovery Module
◦ Windows Passwords: обнаружение учетных данных администратора на серверах и рабочих столах платформы Microsoft. Возможность определять, какие из них являются привилегированными, и импортировать их в хранилище.
◦ Linux / Unix / AIX Passwords: обнаружение учетных данных администратора на серверах и рабочих столах Linux/Unix/Aix. Возможность определять, какие из них являются привилегированными, и импортировать их в хранилище.
◦ AD Passwords: обнаружение учетных данных администратора на сервере Active Directory платформы Microsoft. Возможность определять, какие из них являются привилегированными, и импортировать в хранилище.
◦ SQL / Oracle Passwords: обнаружение учетных данных администратора в базах данных. Возможность определять, какие из них являются привилегированными, и импортировать в хранилище.
◦ SSH Keys: обнаружение открытых и закрытых SSH-ключей, которые присутствуют на целевом устройстве.
◦ Certificates: обнаружение локальных или пользовательских сертификатов Windows, хранящихся на устройствах, контейнерах или в домене.
◦ Local Authorities: обнаружение локальных центров сертификации устройств.
◦ Services: возможность узнать какие службы выполняются на целевом устройстве.
◦ DevOps: обнаружение артефактов DevOps, присутствующих в устройствах.
◦ Glossary of Provisions: возможность создать список сканирования с сегментацией по типу.

Module A2A - App to App

• .Net: доставка пароля через lib на .Net для добавления в код платформы.
• Java: доставка паролей через библиотеку паролей на Java для добавления в код приложения платформы.
• PHP: доставка пароля через библиотеку паролей на PHP для добавления в код приложения платформы.
• Application Server: смена пароля в основных серверах приложений рынка.
• senhasegura API: доставка пароля через Senhasegura API.

Module senhasegura.go

Senhasegura.go позволяет использовать права администратора для запуска приложений на локальных рабочих станциях. Этот модуль основан на .NET Framework для 4.8.

Поддерживаемые интеграции

Senhasegura предоставляет несколько типов интеграции, помимо возможности настройки шаблонов интеграции. Шаблоны могут быть изменены администратором.

Для выполнения интеграции могут потребоваться специальные плагины. Архитектура паролей и функции интеграции позволяют Senhasegura быстро разрабатывать такие плагины.

Senhasegura неинвазивна. Поэтому установка агента в системах, управляемых решением, не требуется. Для некоторых приложений можно использовать Senhasegura через агентов, чтобы создать больше возможностей для интеграции.

Операционные системы

Поставщики	**Версии**
Apple	OS X
Cisco	Cisco IOS, NX-OS (Nexus)
EMC	UNIX
F5	Big IP, LTM
HP	HPUX, Tru64, NonStop (Tandem), Open VMS, HP5500, Tande
IBM	AIX, iSeries, Z/OS, CICS, OS/390
Linux	Fedora, Ubuntu, Red Hat, SUSE Linux, Debian
Microsoft	Windows XP, Windows Vista, Windows 7, Windows 8 / 8.1, Windows 10, Windows Server 2003, 2008, 2012, 2016
NetApp	NetApp
Oracle	Solaris, Solaris Intel, Enterprise Linux
Juniper	JUNOS

Сетевое оборудование

Поставщики	**Оборудование**
3Com	Коммутаторы
A10 Networks	A10
Adtran	NetVanta 838, Tracer 6420
Alcatel	Коммутаторы, Коммутаторы (Omniswitch 7000 Series), Intelligent Services Access Manager (ISAM)
Allot	Allot Secure Service Gateway, Allot Service Gateway, Allot SmartEngage, Allot WebSafe Personal
Applied Innovation	AISCOUT-S02
Aruba Networks	ArubaOS
Avaya	Media Gateway

Поставщики	Оборудование
Avocent	DSView management
BlueCoat	PacketShaper
Brocade	Silkworm
BTI Photonic Systems	NETSTENDER 1030
Cisco	Маршрутизаторы, ACS (Access Control Server), Коммутаторы Catalyst, Коммутаторы Nexus, JMC, Wireless LAN Controller 5508, WAAS, ONS, ESA (Email Security Appliance), Privilege 15, Unified Communication Manager, ISE (Identity Services Engine), UCS (Unified Computing System)
Citrix	Netscaler
Dell	Коммутаторы
Enterasys	Маршрутизаторы, коммутаторы
Ericsson	ServiceOn Element Manager (SOME)
F5	BigIP, LTM
Fujitsu	FSC iRMC
Gemalto	SafeNet KeySecure, SafeNet HSM
HP	ProCurve, HPE 5500
Huawei	S1720, S2700, S5700, S6720, S6720 V200R011C10
Juniper	Маршрутизаторы (JUNOS), Pulse secure
Mcafee	nDLP
Meinberg	Lantime
Netscout	Infinistream
Nokia	NetAct, DX200
Nortel	BayStack, VPN Router, Ethernet Routing Switch
Radware	ISR Infiniband Switch, ODS1 Load Balancer, Alteon, Linkproof
RFL Electronics	IMUX 2000
Riverbed	CMI, Xilinx
RuggedCom	Маршрутизаторы, коммутаторы
Symmetricom	Symmetricom Xli
Voltaire	ISR Infiniband Switch
Extreme Networks	Коммутатор, маршрутизатор
Yamaha	RTX
DLink	Коммутаторы, маршрутизаторы
Foundry	Коммутаторы

Серверы приложений

Поставщики	Серверы
Red Hat	Jboss
Kaspersky	Kaspersky Endpoint Security for Business
Microsoft	SQL Server, Exchange Server 2007 - 2019, entre outras aplicações que permitam interatividade via RemoteApp, Windows RPC e Windows RM, , IIS
Veritas	NetBackup 7.7, 8.0, 8.1 e 8.2
IBM	Websphere Application Server, Websphere Datapower
Apache Foundation	Apache HTTP Server, Apache tomcat
Oracle	WebLogic Server, Peoplesoft, Oracle Application Server

Устройства безопасности (межсетевые экраны, UTMs, IPSs)

Поставщики	Устройства
Acme Packet	Net-Net OS-E
Aker	Aker Firewall UTM
Blue Coat	Proxy SG
Checkpoint	FireWall-1, SPLAT, Provider-1, GAIA
Cisco Systems	PIX, ASA, IronPort, Mail Gateway
Critical Path	Memova Anti-Abuse
Fortinet	FortiGate, Fortimanager
IBM	DataPower Integration Appliance
Juniper	Netscreen
Mcafee	NSM (Network Security Manager), SideWinder, ePO
Nokia	Checkpoint FireWall -1 on IPSO
Palo Alto Networks	Panorama
ProofPoint	Protection Server
RSA	Authentication Manager (SecurID)
Safenet	Luna HSM
Schneider	Industrial Defender
SonicWall	Firewalls
Sophos	Astaro Security Gateway
SourceFire	SourceFire 3D
Symantec	Brightmail Gateway
TippingPoint	IPS, SMS

Поставщики	Устройства
WatchGuard	Firebox X Edge e-series, Firebox X Core e-series, Firebox X Peak e-series, WatchGuard XTM
Imperva	DDoS Protection

Среды виртуализации

Поставщики	Среды
VMware	ESX/ESXi Server
Citrix	Xen Citrix
Microsoft	Hyper-V, Azure
Google	Google Cloud Platform (GCP)
Amazon	Amazon Web Services (AWS)
Rackspace	Rackspace Cloud, GoGrid
IBM	IBM SmartCloud
Generic	ISO installation media

Базы данных

Поставщики	Базы данных
IBM	DB2, Informix, Datastage
InterSystems	Caché Release 2010 - 2017 (и другие поддерживаемые ODBC)
Microsoft	SQL Server
MongoDB	MongoDB
MySQL	MySQL
ODBC	ODBC compatible databases
Oracle	Oracle Database, Oracle Enterprise Manage, RDBMS, Mysql 4 - 8, Oracle RAC
Postgresql	Postgresql 6 - 11
SAP	HANA
Sybase	Sybase Database, IQ

Хранилища

Поставщики	Хранилища
Dell	Dell EMC PowerMax 2000, Dell EMC PowerMax 8000, Dell EMC SC5020, Dell EMC SC5020F, Dell EMC SC7020, Dell EMC SC7020F, Dell EMC SC9000, Dell EMC SCv3000, Dell EMC Unity XT 380F, Dell EMC Unity XT 480F, Dell EMC Unity XT 680F, Dell EMC Unity XT 880F, Dell EMC XtremIO X2, Dell PowerVault, Dell EMC Isilon, Dell EMC VMAX Среди других моделей, совместимых с поддерживаемыми соединениями
IBM	Storwize V7000 Gen 3 ”Next Gen”, Storwize V7000 Gen 2+, Storwize V7000 Gen 2, Storwize V7000 family, Storwize V5100E, Storwize V5030E, Storwize V5010E, Storwize V5030, Storwize V5020, Storwize V5010, Storwize V5000

Поставщики	Хранилища
Huawei	OceanStor 18000F V5, OceanStor 5300 V3, OceanStor 5300F, OceanStor 5500 V3, OceanStor 5500F, OceanStor 5600 V3, OceanStor 5600F , OceanStor 5800 V3, OceanStor 5800F V5, OceanStor 6800 V3, OceanStor 6800F V5 Среди других моделей, совместимых с поддерживаемыми соединениями
NetApp	NetApp ONTAP (BSD)
Hitachi	Enterprise Storage, séries E, F, G e 5.000
Pure Storage	File Storage

Приложения Windows

Приложения, разработанные под Java, .Net, PHP, Phyton, учетные записи SQL, Планировщик задач Windows, службы Windows, приложения Apache, приложения IIS, службы COM+, кластерные приложения

Системы каталогов

Поставщики	Системы
Digi	Digi Remote Manager
Fujitsu	iRMC
Microsoft	ActiveDirectory
Novell	Novell Directory Services (NDS)
Sun	Java System Directory Server
Red Hat	Red Hat Directory Server (RHDS), 389 Directory Server, FreeIPA
Oracle	ODI Oracle

Удаленный доступ и мониторинг

Поставщики	Модели
Amazon	Amazon Web Services (AWS)
Dell	Dell Remote Access Card (DRAC)
HP	StorageWorks, iLO
CA Technologies	CA Remote Control
IBM	Maximo Application Suite
SUN Technologies	Desktop Management
Digi	Digi Remote Manager
Cyclades	Cyclades-TS
Fujitsu	ServerView Suite

Среды DevOps, VSC и другое программное обеспечение SDLC

Поставщики	Модели
Ansible	Ansible
Atlassian	Bamboo CI/CD, JIRA Core, Bitbucket
GitLab Inc.	GitLab CI/CD
Google	Kubernetes
Jenkins	Jenkins CI/CD

Инструменты управления ИТ-услугами

Поставщики	Инструменты
Atlassian	Jira Service Desk
Zendesk	Zendesk
Freshworks	Freshdesk
ServiceNow	ServiceNow ITSM
GLPI	ITSM GLPI

TOTP-инструменты

Senhasegura работает с любым инструментом генерации одноразового пароля на основе времени (TOTP).
Ниже представлены только несколько вариантов:

Поставщики	Инструменты
Google	Google Authenticator
Microsoft	Microsoft Authenticator
Authy	Twilio Authy 2-Factor Authentication
Red Hat	FreeOTP Authenticator
Sophos	Sophos Authenticator
LastPass	LastPass Authenticator
andOTP	andOTP

Плагины интеграции

Интеграция	Функция
Jenkins	Позволяет получить доступ к секретам в Senhasegura

SIEM-решения

Поставщики	Версии
Exabeam	Версия i 31 и выше
IBM QRadar	Версия 7.3 и выше
LogRhythm	Версия 7.4 и выше
Rapid7 - InsightIDR	Версия 20180814 и выше
Rapid7 - InsightOps	Версия 20190204 и выше
Securonix	Версия 6.3 и выше
Splunk	Версия 6.3 и выше

SSO-решения

Поставщики	Решения
Okta	Lifecycle Management
RSA	RSA SecurID
Duo	Duo Multi-factor Authentication
Red Hat	Keycloak

Интеграции аутентификации

SSO

Инструменты	Протокол	Интеграция
Active Directory	LDAP	Полная
Azure AD	SAML 2.0	Полная
ForgeRock	SAML 2.0	Полная
Google	OpenID	Полная
AuthID	OpenID	Полная
Keycloak	OpenID SAML 2.0	Полная
Okta	OpenID SAML 2.0	Полная

MFA

Инструменты	Протокол	Интеграция
Duo	TOTP OpenID	Полная
Email	TOTP	Частичная
Google Authenticator	TOTP	Полная
Microsoft Authenticator	TOTP	Полная
Okta	TOTP OpenID	Частичная

Инструменты	Протокол	Интеграция
RSA		Полная
SmartCards	A3 x.509	Частичная
SMS	TOTP	Частичная
Symantec VIP	TOTP	Полная
Tokens	A3 x.509	Частичная

Версия встроенного браузера

Firefox 91.6.1esr (64-бит)

Функции шифрования и безопасности

Шифрование

Библиотека OpenSSL, поддерживаемая OpenSSL Software Foundation, представляет собой реализацию криптографических протоколов SSL и TLS с открытым исходным кодом. В библиотеке реализованы основные алгоритмы шифрования на языке программирования C. Senhasegura использует криптографическую библиотеку OpenSSL для выполнения всех криптографических процессов, необходимых для работы решения. Библиотека OpenSSL шифрует всю информацию, хранящуюся в базе данных, поэтому все данные, используемые Senhasegura, защищены от несанкционированного доступа. Вся связь между компонентами решения использует протокол SSL (Secure Sockets Layer) для шифрования передаваемых сообщений.

Библиотека OpenSSL сертифицирована по стандарту FIPS 140-2. Узнать больше по ссылке:
https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security- policies/140sp4282.pdf

Для компаний, которым требуется более высокий уровень безопасности, Senhasegura предлагает PAM Crypto Appliance и интеграцию с основными HSM на рынке, таким образом, придерживаясь стандартов безопасности FIPS 140-2 уровня 2 и выше. Для аутентификации в веб-интерфейсе Senhasegura — как локально, так и через внешние серверы аутентификации — все пароли пользователей хранятся в формате хэшей SHA-256. Связь между рабочей станцией клиента и Senhasegura осуществляется посредством зашифрованной связи с соблюдением стандартов шифрования используемых протоколов. Независимо от канала связи, будь то RDP, SSH или HTTPS

Доступ к удаленным целевым устройствам соответствует одному и тому же стандарту шифрования во всех протоколах, допускающих настройку.

Стандарты безопасности

- FIPS 140-2
- Другие

HSM-шифрование

Для компаний, которым требуется более высокий уровень безопасности, вы можете выбрать аппаратный безопасный модуль (HSM), аппаратное устройство безопасности и шифрования с военными спецификациями и стандартами защиты от несанкционированного доступа.

Технические характеристики HSM

- Шифрование
- RSA (PKCS #1 V2.1) (1024, 2048, 4096 бит)
- ECDSA (NIST FIPS PUB 186-3)
- FIPS 197 AES 128, 192, 256
- FIPS 46-3 DES/3DES
- Поддержка сертификатов x509v3
- Поддержка импорта и внутренней генерации ключей
- Генератор случайных чисел
- Внутреннее аппаратное обеспечение соответствует стандарту AIS31 P2
- Real time clock (RTC)
- Внутреннее, максимальное отклонение 1 минута в год
- Устройство и функции безопасности устройства
- HSM Entrust nShield
- HSM Kryptus
- HSM Thales
- HSM GEMALTO
- HSM DINAMO
- HSM YUBICO

Шифрование веб-прокси

- Методы обмена ключами:
  - ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521
  - ssh-curve25519-sha256
  - ssh-curve25519-sha256-libssh
  - diffie-helman-group-exchange-sha256 diffie-helman-group-exchange-sha1 diffie-helman-group14-sha1
  - diffie-helman-group1-sha1
- Поддерживаемые ключи:
  - ecdsa-ssh-nistp256 ecdsa-ssh-nistp384 ecdsa-ssh-nistp521 ssh-ed25519
  - ssh-rsa ssh-dss
- Методы MAC:
  - hmac-sha2-256
  - hmac-sha2-512
  - hmac-sha1
  - hmac-sha1-96
  - hmac-md5
  - hmac-md5-96
  - hmac-ripemd160
  - hmac-ripemd160-openssh-com
- Шифры
  - aes128-ctr aes192-ctr aes256-ctr aes256-cbc
  - rijndael-cbc-lysator-liu-se aes192-cbc
  - aes128-cbc blowfish-cbc arcfour128 arcfour cast128-cbc 3des-cbc

Шифрование прокси терминала

- Методы обмена ключами:
  - ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521
  - diffie-hellman-group16-sha512
  - diffie-hellman-group-exchange-sha256 diffie-hellman-group14-sha256
  - diffie-hellman-group-exchange-sha1 diffie-hellman-group14-sha1
  - diffie-hellman-group1-sha1
- Поддерживаемые ключи:
  - ssh-ed25519
  - ecdsa-sha2-nistp256 ecdsa-sha2-nistp384 ecdsa-sha2-nistp521 ssh-rsa
  - ssh-dss
- Методы MAC:
  - hmac-sha2-256
  - hmac-sha2-512
  - hmac-sha2-256-etm@openssh.com
  - hmac-sha2-512-etm@openssh.com
  - hmac-sha1
  - hmac-md5
  - hmac-sha1-96
  - hmac-md5-96
- Шифры:
  - aes128-ctr
  - aes192-ctr
  - aes256-ctr
  - aes128-cbc
  - aes192-cbc
  - aes256-cbc
  - blowfish-cbc
  - 3des-cbc

Шифрование сессий SSH

Симметричные шифры

- 3DES
- AES128-cbc
- AES192-cbc
- AES256-cbc
- rijndael-cbc
- AES128-ctr
- AES192-ctr
- AES256-ctr
- AES128-gmc
- AES256-gmc
- chacha20-poly1305

Симметричные шифры, поддерживающие аутентифицированное шифрование

- AES128-gmc
- AES256-gmc
- chacha20-poly1305

MAC

- hmac-sha1
- hmac-sha1-96
- hmac-sha1-256
- hmac-sha1-512
- hmac-md5
- hmac-md5-96
- umac-64
- umac-128
- hmac-sha1-96-etm
- hmac-sha1-256-etm
- hmac-sha1-512-etm
- hmac-md5-etm
- hma-md5-96-etm
- umac-64-etm umac-128-etm

Алгоритмы обмена ключами

- diffie-hellman-group1-sha1
- diffie-hellman-group14-sha1
- diffie-hellman-group14-sha256
- diffie-hellman-group16-sha512
- diffie-hellman-group18-sha512
- diffie-hellman-group-exchange-sha1
- diffie-hellman-group-exchange-sha256
- ecdh-sha2-nistp256
- ecdh-sha2-nistp384
- ecdh-sha2-nistp521
- curve25519-sha256

Ключ сертификата

- ssh-ed25519-cert-v01
- ssh-rsa-cert-v01
- ssh-dss-cert-v01
- ecdsa-sha2-nestp256-cert-v01
- ecdsa-sha2-nestp384-cert-v01
- ecdsa-sha2-nestp521-cert-v01

Типы ключей

- ssh-ed25519
- ssh-ed25519-cert-v01
- ssh-rsa
- ssh-dss
- ecdsa-sha2-nestp256
- ecdsa-sha2-nestp384
- ecdsa-sha2-nestp521
- ssh-rsa-cert-v01
- ssh-dss-cert-v01
- ecdsa-sha2-nestp256-cert-v01
- ecdsa-sha2-nestp384-cert-v01
- ecdsa-sha2-nestp521-cert-v01

Доступность и чрезвычайные ситуации

Система Senhasegura поддерживает работу на виртуальных или физических устройствах. Виртуальное устройство Senhasegura настроено для установки без отключения пользователей-администраторов в операционной системе.
В любой конфигурации система поддерживает настройки для высокой доступности и угроз внешних чрезвычайных ситуаций.

Резервное копирование

Senhasegura предоставляет несколько механизмов для восстановления информации в случае сбоя:

Резервное копирование зашифрованного пароля

Внешнее копирование в клиентской инфраструктуре. Резервный файл с этой информацией защищен паролем, который распространяется на многократное хранение среди доверенных участников по свободному выбору клиента. Для получения и извлечения информации требуется как минимум два пользователя-хранителя. После доставки Senhasegura все пароли к сейфу будут сброшены, и клиент получит их соответствующее хранение, за исключением паролей к базе данных Senhasegura и операционной системе.
Начиная с версии 3.10 процедура резервного копирования также будет выполняться для пользовательских паролей и ключей доступа модуля DevSecOps.

Быстрое восстановление резервного копирования

Внутреннее и быстрое восстановление. Такой вид копирования обеспечивает хранение большего объема критической информации и считается более быстрым. Так как при наличии базового содержимого среда восстанавливается быстро и становится доступной уже по запросу.

Зашифрованное резервное копирование настроек

Благодаря этому типу копирования не только сохраненные данные, но и настройки пароля могут быть доступными для извлечения. Этот тип резервного копирования не включен по умолчанию, но его активация доступна в настройках системы.

Безопасное резервное копирование видео

Senhasegura позволяет сохранять резервные копии видео в удаленном каталоге под ответственность клиента. По умолчанию видео хранятся в файловой системе решения.

Резервное копирование секретов

Резервное копирование секретов: console credentials и access keys хранятся в выделенных каталогах.

Мониторинг, системный журнал и SIEM

Senhasegura имеет возможности мониторинга, предназначенные для оповещения администраторов о любом процессе, интеграции, подключении или сбое доступа.

Система отправляет оповещения администратору на экран, по электронной почте или SMS, snmpmibs и snmptraps.

Решение может быть интегрировано с любым отраслевым инструментом с использованием стандарта SNMP V1, V2 или V3.
Интеграция с сервисами Syslog и SIEM.

Собственная интеграция с ArcSight.

Совместимость с браузерами

Веб-интерфейс Senhasegura доступен только по протоколу HTTPS, и мы рекомендуем предоставить собственный сертификат SSL в соответствии с действующими на рынке предположениями о безопасности.

Senhasegura использует технологии HTML5 и WebSocket, и только браузеры, поддерживающие эти технологии, обеспечат полную защиту паролей. Решение также поддерживает совместимость со следующими браузерами в их самых последних версиях:

- Internet Explorer
- Google Chrome
- Microsoft Edge
- Mozilla Firefox

Условия работы сети

Соединения между пользователями и приложением Senhasegura имеют минимальную пропускную способность 180 Кбит/с на удаленную сессию без потери функциональности.

Соединения между пользователями и приложением Senhasegura имеют максимальную задержку 900 мс без потери функциональности.

Приложение Senhasegura позволяет поддерживать протоколы IPV4 и IPV6 в соответствии со спецификацией IETF RFC 2460.

Поддерживаемые протоколы и порты

Senhasegura позволяет использовать несколько протоколов через соответствующие стандартные порты или любые другие, настроенные в решении, для следующих операций: удаленные подключения, изменение пароля, Scan Discovery, аутентификация и доступ в интернет.

Операции выполняются на основе портов, настроенных на устройстве.

Соединение	Порт по умолчанию	Описание
HTTP	80	Веб-доступ
HTTPS	443	Защищенный веб-доступ
LDAP	389	Scan Discovery / Аутентификация
LDAPS	636	Смена пароля / Scan / Discovery / Аутентификация
MySQL	3306	Удаленное подключение* / смена пароля
Oracle	1521	Удаленное подключение* / смена пароля
PostgreeSQL	5432	Удаленное подключение* / смена пароля
RDP *	3389	Удаленное подключение
RM HTTP	5985	Смена пароля / Scan Discovery
RM HTTPS	5986	Смена пароля / Scan Discovery
SQL Server	1433	Удаленное подключение* / смена пароля
SSH	22	Удаленное подключение / смена пароля
Telnet	23	Удаленное подключение / смена пароля
VNC **	5900	Удаленное подключение
Windows RM	5986	Смена пароля
Windows RPC	135	Смена пароля / Scan Discovery
X11 Forward **	22	Удаленное подключение / изменение пароля

Поддерживаемые протоколы доступны только для TLS1.2 и TLS1.3 после подключения к хранилищу Senhasegura.

* только RemoteApp
** графические интерфейсы

Производительность

Архитектура Senhasegura рассчитана на максимальную производительность во всех операциях, выполняемых с помощью решения.

Все тесты на Senhasegura PAM Crypto Appliance проводились со следующей конфигурацией:

Настройки оборудования

- Версия: Senhasegura PAM Crypto Appliance Titanium
- Процессор: Intel E5-2630v4
- Оперативная память: 128 Гб
- Жесткий диск: 2x2TB NLSAS RAID1

Настройки Senhasegura

- Процессор: 38 vCPUs
- Оперативная память: 126 Гб
- Жесткий диск: 2 Тб

Сессии SSH через терминальный прокси Senhasegura

Соединения	ЦПУ	ОП	ДИСК W
500	5%	10 Гб	4.500 КБ/с
2000	20%	50 Гб	6.000 КБ/с
3500	55%	85 Гб	8.000 КБ/с

Сессии SSH через Senhasegura веб-прокси

Соединения	ЦПУ	ОП	ДИСК W
250	10%	10 Гб	2.000 КБ/с
750	35%	15 Гб	5.000 КБ/с
1250	45%	20 Гб	7.500 КБ/с

Сессии RDP через Senhasegura RDP Proxy

Соединения	ЦПУ	ОП	ДИСК W
500	5%	15 Гб	2.000 КБ/с
1250	10%	30 Гб	5.000 КБ/с
2000	15%	50 Гб	8.500 КБ/с

Сессии RDP через Senhasegura веб-прокси

Соединения	ЦПУ	ОП	ДИСК W
250	5%	10 Гб	1.000 КБ/с
1000	10%	20 Гб	9.000 КБ/с
1750	20%	30 Гб	16.000 КБ/с

Веб-соединения HTTP (высокая нагрузка)

Соединения	ЦПУ	ОП	ДИСК W
10	10%	5 Гб	1.500 КБ/с
20	18%	10 Гб	1.800 КБ/с
30	20%	15 Гб	2.100 КБ/с

Веб-соединения HTTP (средняя нагрузка)

Соединения	ЦПУ	ОП	ДИСК W
10	10%	4 Гб	10.000 КБ/с
20	20%	8 Гб	40.000 КБ/с
30	20%	10 Гб	80.000 КБ/с

Веб-соединения HTTP (низкая нагрузка)

Соединения	ЦПУ	ОП	ДИСК W
10	10%	10 Гб	10.000 КБ/с
35	20%	15 Гб	20.000 КБ/с
60	30%	20 Гб	40.000 КБ/с

Лимит ресурсов

Платформа Senhasegura имеет несколько функций, которые технически ограничены по причинам ограничений базы данных, ограничений операционной системы, ограничений файловой системы или ограничений архитектуры программного обеспечения.

Ограничения, связанные с контрактом или лицензией, устанавливаются контрактом и не будут рассматриваться в этом разделе.

Ограничения, связанные с количеством контрактных экземпляров в кластерном сценарии, также не будут рассматриваться в этом разделе. Мы сосредоточимся на ограничениях экземпляра и его компонентов.

Лимит пользователей

Технически приложение может поддерживать до 16 500 000 записей пользователей. Данный лимит распространяется на пользователей WebService A2A, пользователей служб и фактических пользователей системы. Это число не отражает возможности одновременного использования системы всеми этими пользователями. Емкость одновременного использования может варьироваться в зависимости от типа использования, количества контрактных экземпляров и предоставляемой сетевой задержки.

Лимит устройств

Технически приложение поддерживает до 16 500 000 записей устройств. В это число входят даже деактивированные устройства. Данный лимит не отражает возможность доступа ко всем этим устройствам через прокси или любой другой асинхронный процесс, который одновременно обращается к устройству. Возможность управления устройствами может зависеть от количества контрактных экземпляров, поддерживаемых систем и протоколов, а также предоставляемой сетевой задержки.

Лимит учетных данных и защищенная информация

Технически приложение может поддерживать до 16 500 000 учетных записей. Этот лимит распространяется даже на учетные данные, ставшие неактивными с течением времени. Это число не означает, что все эти учетные данные доступны и используются асинхронными задачами или прокси-сессиями одновременно. Возможность управления учетными данными зависит от количества контрактных экземпляров и предоставляемой сетевой задержки.

Запись прокси-сессии

В отличие от других решений на рынке, Senhasegura не выполняет захват экрана в формате изображения или видео в реальном времени в формате mp4 или других медиаформатах. Реальное постоянство протокола обеспечивает точную и оптимизированную копию сессий. Время бездействия записывается с помощью меток времени 4 байта в секунду, в отличие от захвата экрана, который потребляет гораздо больше ресурсов. Запись протокола в собственном формате уже учитывает собственный формат сжатия протокола.

Видео сессии зашифровано и хранится в собственном формате и на том же сервере, что и пароль, со всеми стандартными средствами защиты хранилища, обеспечивающими целостность видео. Если заказчик хочет применить собственные стандарты безопасности, он может настроить внешнее резервное копирование.

Поведение пользователя будет определять количество сессий, которые можно сохранить. Не исключая возможности расширения диска или подключения удаленного хранилища для увеличения емкости хранилища.

Такое сочетание факторов делает лимит сессий практически неограниченным. Обратитесь к таблице производительности, описанной в производительности сессии, чтобы рассчитать свою потребность.

Одновременные прокси-сессии

Количество одновременных сессий может варьироваться в зависимости от количества контрактных экземпляров, что делает решение соответствующим вашим потребностям без чрезмерного приобретения ресурсов. Кластерная архитектура также позволяет определять выделенные узлы для конкретных протоколов или определять выделенные экземпляры для разных центров обработки данных или сегментов сети. Такое сочетание факторов делает лимит сессий практически неограниченным. Обратитесь к таблице производительности, описанной в разделе производительности, чтобы рассчитать свои потребности.

Версии Senhasegura

Номенклатура версий Senhasegura соответствует формату M. N.P. (например, 3.22.1-9)

Тип обновления	**Описание**
M - Общее	Включает глубокие архитектурные и/или технологические изменения.
N – дополнительные компоненты	Включает новые функции и/или улучшения существующих функций. Также включает известные исправления ошибок и незначительные архитектурные изменения.
P – критическое	Включает исправления критических ошибок и исправления безопасности (рекомендуется немедленное обновление).

Как часто выходят новые версии

Частота обновлений Senhasegura может варьироваться от 1 до 5 месяцев, в зависимости от периода года.

Что касается доступных форматов, есть два варианта:

- Для новой среды Senhasegura можно использовать виртуальные машины, доступные в службе поддержки партнеров
- Обновления всегда доступны в наших репозиториях, а новые выпуски обновляются, как только они становятся доступными

Требования к установке

Сценарии использования

Для корректного функционирования решения необходимо определить возможные сценарии использования, в которых будет выполняться управление привилегированным доступом.

Ниже вы можете найти несколько вариантов использования:

- **Active Directory**: администратор Active Directory хочет иметь доступ к удаленному рабочему столу (RDP) к серверу Active Directory Server Windows Server 2016 с использованием пользователя «Администратор».

- **Databases**: администратор базы данных хочет иметь доступ к программному клиенту SQL Server Management Studio 2014, который управляет базой данных SQL, используя пользователя локального администратора производственного экземпляра базы данных «sa».
- **Network Assets**: администратору инфраструктуры требуется доступ через командную строку, оболочку или консоль к маршрутизатору Cisco, через порт SSH или Telnet, используя пользователя «Оператор» или «Администратор».
- **Web Applications**: доступ к порталу AWS, используя учетную запись администратора облачных вычислений, используя учетную запись «senhasegura@gmail.com».
- **Deletion of credentials in hardcode**: если вы хотите удалить учетные данные базы данных, записанные в исходном коде приложения для учета, измените пароль, синхронизированный в файлах конфигурации и службах, зависящих от аутентификации, или предоставьте API подключения для вашей подписки.
- **Registration of Activities with Generic Users**: запись о действиях во время любой сессии, включая журналы пользовательского аудита, искать любую команду, выполняемую с клавиатуры во время сессии и в записях.
- **Segregation of Functions and Segmentation of Functions**: вы хотите создать профили пользователей, разбитые по спискам запрещенных команд, использующие одни и те же привилегированные учетные данные. Вы хотите определить группы с привилегированным доступом к связанным пользователям, принадлежащим к той же области.
- **VPNs Optimization**: вы хотите контролировать и отслеживать в режиме реального времени доступ поставщиков и сторонних пользователей к корпоративной среде, предоставлять удаленный доступ только к определенным приложениям или сервисам в сети на заранее установленное время.
- **Cloud Environment Recording**: вы хотите управлять доступом к облачным приложениям и обеспечивать легитимность пользователей, которые будут подключаться к тем же стандартам управления ИТ, что и все другие внутренние сетевые среды.
- **Shared Access**: с критически важными приложениями, лицензирование которых очень дорого, Senhasegura может предоставить общий неодновременный доступ из нескольких мест для разных пользователей, используя одни и те же привилегированные учетные данные, получая независимую и персонализированную информацию для каждой сессии и записи видео.
- **Repository for Strength Analysis**: анализ поведения, чтобы получить показатели, отчеты об использовании модели, планирование инвентаризации и структурирование политики для эффективного использования ресурсов. Онлайн-доступ к записям сессий для устранения неполадок.
- **Information Protection**: хранение информации с цифровыми сертификатами, ключами подключения, ключами шифрования и паролями личного доступа, с помощью которых вы можете определять потоки и элементы управления доступом, которые свидетельствуют и отслеживают их использование и визуализацию.

Требования в управляемых системах

Определите следующую информацию для управляемых систем:

- Имя хоста: имя хоста устройства. Оно будет идентификатором запросов. (Например, apl001s10 или Facebook).

- Управление IP: IP-адрес управления устройством, используемый хранилищем для подключения. (Например, 192.168.10.1 или facebook.com).
- Производитель: производитель устройства. Он будет создан, если вы не зарегистрированы. (Например, Microsoft, Oracle).
- Тип: тип устройства. Он будет создан, если вы не зарегистрированы. (Например: server, Subscription)
- Модель: модель устройства. Она будет создана, если вы не зарегистрированы. (Например, Windows Server 2012).
- Местоположение: географическое положение. Где находится устройство. Он будет создан, если вы не зарегистрированы. (Например, ЦОД Гватемала).
- Дополнение 1: дополнительная информация. (Например, Platform, Core, Accounting).
- Дополнение 2: дополнительная информация. (Например, System, Database, Data, Main Application)
- Подключение: подключение устройства и шлюза, разделенные запятой и двоеточием. (Например: RDP: 3389, SSH: 22).
- Домен: домен устройства. (Например, domain.com)

Требования к привилегированной учетной записи

Чтобы получить доступ к управляемым системам, вы должны иметь следующую информацию из учетных данных или привилегированных учетных записей:

- Password Type: политика паролей (Например, local user Privileged)
- User: имя пользователя (Например: root).
- Password: значение пароля. Если это поле не заполнено, пароль не обновится. (Например, Da@lU!83m$1).
- Domain: домен учетной записи (Например, domain.com).
- Additional information: дополнительная информация о текущем удостоверении. Используется для экземпляров БД, смены пароля или ссылок в целом. (Например, ORAC19).
- Labels: метки пароля, разделенные запятыми. Они используется для группировки или фильтрации определенных учетных данных. (Например: cellphone, dev)
- Enable Auto Change: указать, будет ли пароль автоматически изменен хранилищем (Да или Нет).
- Swap plugin: плагин, используемый в модели изменения. (Например: NetSSH)
- Change Template: шаблон для смены пароля. (Например, Linux as root)
- Status Control: указывает, будет ли статус пароля автоматически контролироваться хранилищем. (Да или Нет)
- Plugin activation: плагин, используемый моделью активации. (Например: Net SSH)
- Activation model: модель, используемая для активации учетных данных. (Например: Enable credentials as root)
- Plug-in inactivation: плагин, используемый моделью деактивации учетных данных. (Например, Net SSH)
- Inactivation model: шаблон, используемый для выполнения деактивации учетных данных. (Например: Disabling credentials as root)
- User for connection: пользователь, используемый для подключения к оборудованию и выполнения изменений состояния и операций управления. Вы можете использовать те же учетные данные. (Например: root or even password)
- Hostname for connection: имя хоста, используемое для подключения к устройству и выполнения операций управления и изменения состояния. Вы можете использовать то же значение пароля. (Например, apl001s10 или Even of the password).
- Credential owner: пользователь учетной записи.

Требования к группам доступа и пользователям

Чтобы запустить хранилище Senhasegura и определенные привилегированные учетные записи, необходимо создать группы доступа. Они позволят применять фильтры по сегментам или группам, различным управляемым системам, привилегированным учетным записям и привилегиям, для которых пользователи должны иметь свои собственные учетные данные доступа. Вы можете создать их локально в хранилище или интегрировать с источником аутентификации, таким как Active Directory, Radius или TACACS, для настройки этих функций:

Требования:

- Number of Access Groups
- Names of Access Groups
- Systems Privileged by Access Groups
- Privileged Accounts by Access Groups
- Users by Access Groups
- Options by Access Groups (Доступ к сессий и просмотр пароля должны быть установлены, если вам нужно ввести причину или получить одобрение)
- Access limitations by days of the week and time slots (8:00 -12:00, 12:00 - 16:00, 16:00 - 20:00, 20:00 - 00:00, 00:00 - 04:00, 04:00 - 08:00).

Пример заполнения поля группы доступа:

Имя	Система	Привилегированные УЗ	Пользователи	Опции	Ограничения доступа
Servers	SRV Win 2016 (10.235.x.x)	Administrator	a.martinez	только доступ к сессии без запроса или одобрения	Каждый день с 8:00 до 17:00

При росте числа пользователей и устройств, определенных изначально, решение должно быть рассчитано с запасом в 20%, чтобы расти без необходимости модификации оборудования. Если рост более значительный, всегда можно масштабировать решение, интегрируя его с другим оборудованием с превосходящими возможностями.

Профили пользователей в Senhasegura

Чтобы решение работало по назначению, мы рекомендуем иметь следующие профили доступа:

- **Administrator**: пользователь с более высокими привилегиями в хранилище, отвечающий за действия по настройке, изменение и устранение любой конфигурации во время ее работы. Рекомендуется, чтобы существовал только один профиль администратора, и чтобы любая деятельность, выполняемая им, была предварительно задокументирована и авторизована.
- **Configurator**: пользователь с высокими привилегиями в хранилище, ответственный за привилегированную учетную запись или действия по модификации системы, которыми он управляет. Рекомендуется, чтобы было не менее двух пользователей с профилем Configurator и чтобы любое выполняемое ими действие было предварительно задокументировано и авторизовано.
- **Auditor**: пользователь с правами только на просмотр записей сессий и их журналов аудита. У этого профиля может быть несколько пользователей,

которые могут быть частью персонала компании или сторонними подрядчиками.
- **User with privileged access**: пользователи только с сессионным доступом к управляемым системам, которые используют привилегированные учетные данные, определенные в группе доступа, к которой принадлежит пользователь. Можно настроить столько пользователей, сколько разрешено в пользовательской лицензии.
- **View of user with a privileged password**: пользователь с доступом для просмотра пароля привилегированной учетной записи управляемых систем, определяемой группой доступа, к которой принадлежит пользователь. Можно настроить столько пользователей, сколько разрешено в пользовательской лицензии.
- **User with privileged access and view**: пользователь с привилегированным доступом, режимом входа в систему, паролем для управляемых систем и привилегированные учетные данные, определяемые группой доступа, к которой принадлежит пользователь. Можно настроить столько пользователей, сколько разрешено в пользовательской лицензии. В этом профиле может быть несколько пользователей. Они могут быть частью персонала компании, приложений или сторонними подрядчиками.

Пример заполнения полей пользователя:

Имя	Имя пользователя	Отдел	Email	Телефон	Группа доступа	Профиль
Alex Martinez	a.martinez	Administration	alex.m@gmail.com	+000 000XXXX	Servers	Пользователь с привилегированным доступом

Требования к виртуальным устройствам PAM

Совместимость

Вы можете реализовать Senhasegura в виртуализированных средах. Требования к виртуализации зависят от решения, используемого для развертывания, и необходимых устройств. В соответствии с определенной архитектурой совместимыми средами являются следующие:

- VMware® (ESX/ESXi Server): поддержка ESXi 7.0 и ESXi 6.x (OVA deployment), необходимо использовать драйвер сетевого адаптера VMXNET3, а также паравиртуализированный диск. При развертывании виртуальной машины (ВМ) обновление должно выполняться на оборудовании машины. Можно использовать виртуальные машины в формате OVA/OVF.
- Xen Citrix®: поддержка Citrix Hypervisor 8.2 LTSR, Citrix XenServer 7.0, XenServer 7.1 LTSR, и Xen Project 4.x.x Series (развертывание OVA). Вы должны использовать генератор HVM. Можно использовать виртуальные машины формата RAW.
- Microsoft® Hyper-V: поддержка Windows Server 2019, Windows Server 2016, Windows Server 2012, и Windows 10 (преобразование OVA в VHD), можно использовать виртуальные машины в формате VHD/VHDx. Azure: можно использовать виртуальные машины в формате VHD. AWS: виртуальная машина в структуре OVA или VMDK.

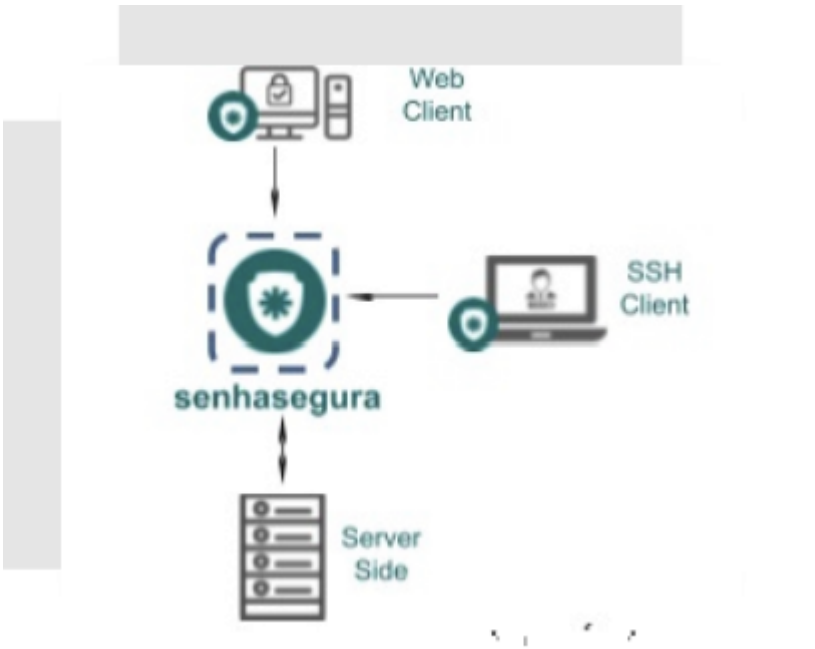
- Microsoft® Azure (преобразование OVA в VHD).
- Linux KVM(QCOW2).
- Amazon (Amazon Web Services - AWS) (развертывание AMI) (введите ID аккаунта и регион).
- Google® Cloud Platform (GCP) (развертывание OVA).
- Openstack: можно использовать виртуальные машины в формате RAW.
- ISO installation media.

Требования к оборудованию

Данные требования зависят от максимального количества одновременных сессий, обрабатываемых решением, и времени хранения записи, заданного каждым сценарием в различных средах, которые определяются в соответствии со следующей информацией:

- RDP/SSH: когда доступ осуществляется прокси-сервером терминала.
- Web: когда доступ осуществляется через браузер.

Структура доступа выглядит следующим образом:



Потребление на соединение

Оборудование	Нагрузка	RDP/SSH	Веб
ЦПУ: количество одновременных подключений на ядро (подк./ядро)	Умеренная	300	30
ОП: объем памяти, используемый на одно соединение (Мб/подк.)	Умеренная	20	40
ЖД: место на диске по времени на соединение (Кб/с/подк.)	Умеренная	3	4

Сетевой трафик на соединение	(Сторона сервера RX / TX)	(кбит/с / подк.)
Умеренный	1/3	45/5

Сетевой трафик на соединение	(Сторона клиента RX / TX)	(кбит/с / подк.)
Умеренный	0.2/1.0	10/80

Для архитектуры высокой доступности (Active-Passive) с двумя элементами в кластере необходимы две машины с точными требованиями к оборудованию. Для модели (Active-Active) необходимо добавить балансировщик, который не входит в комплект.

Требования к оборудованию RDS сервера (только если применимо)

Если нужно определить сессии с сегментированными приложениями в средах Windows (выделенные программные клиенты, промежуточные базы данных и т. д.), вам необходимо внедрить сервер служб удаленных рабочих столов (RDS), лицензирование и внедрение которого не покрываются Senhasegura. Доступность функций для этой услуги требования к доступности оборудования и лицензии должны быть умножены на количество функций: Службы удаленного рабочего стола.

Приложения должны быть опубликованы с этого сервера, после чего Senhasegura будет использовать API удаленных приложений для использования службы. Размер этого сервера зависит от количества конкретных параллельных серверов для этого типа сессии: Узлы сессий удаленного рабочего стола.

Мы рекомендуем приобрести этот сервер по крайней мере с одной операционной системой Windows Server 2008 R2 и с лицензиями на пользователя или сервер, которые должен предлагать производитель: «RDS Per User CAL». Ссылка на производителя с информацией о лицензировании: Удаленный рабочий стол клиентская лицензия доступа.

Что касается аппаратного обеспечения, необходимого для работы производимого сервера, существует таблица уровней функциональной нагрузки объектов.

У производителя есть руководства по реализации этой функции с информацией о ней: Рекомендации для виртуальной машины удаленного рабочего стола.

Исходя из всего вышеизложенного, в случае с клиентами мы рекомендуем оценить количество вариантов использования, требующих сегментированного доступа для каждого приложения, при этом мы имеем количество одновременных пользователей и успеваем получить необходимые требования к оборудованию для сервера RDS, который должен быть установлен на месте.

Версия #2
Денис Морозов создал 30 марта 2023 22:34:40
Денис Морозов обновил 18 апреля 2023 17:49:08