РУТОКЕН

AVANPOST

Комплексная аутентификация: как Рутокен и Аванпост обеспечивают безопасность вашего бизнеса

Андрей Шпаков

Руководитель направления многофакторной аутентификации, Компания «Актив»

Дмитрий Грудинин

Руководитель по развитию продуктовой линейки аутентификации Avanpost FAM/MFA+, Avanpost

Почему традиционные методы защиты данных уже не работают?

94%

повторно используют
слабые пароли

Проблема «пароля по умолчанию»

Преимущества аппаратных аутентификаторов

Рутокен – современные отечественные аутентификаторы, использующие технологии PKI, TOTP и FIDO2

#1 Высокий уровень безопасности

Устойчивость к клонированию, реверс-инжинирингу, атакам на оперативную память

#2 Кроссплатформенность

Работают на всех платформах и ОС

#3 Дополнительные проверки

Биометрическая верификация, сенсорная кнопка и т.д.

#4 Широта интеграций

Легко интегрируется с другими решениями

#5 Четкое понимание расходов

Один пользователь — одно устройство

Популярные сценарии

Вход на рабочие станции Windows, Linux, доменные учетные записи ОС

Вместо ввода пароля от учетной записи, пользователь подключает устройство Рутокен ЭЦП и вводит PIN-код от него. При отключении устройства активная сессия блокируется.

Дополнительная аутентификация через OTP в корпоративные сервисы

Рутокен OTP позволяет сгенерировать одноразовый пароль, который вводится в дополнение к учетным данным пользователя.

Защита удаленного доступа

Для подключения по VPN необходимо использовать токен и ввести PIN-код.

Защита рабочих станций

Рутокен ЭЦП выступает в качестве аппаратного идентификатора в средствах защиты от несанкционированного доступа и модулях доверенной загрузки.

Универсальная карта сотрудника

Одна карта сотрудника Рутокен ЭЦП – пропуск входа в помещения через СКУД и аутентификатор в информационные системы.

Защита веб-приложений

Рутокен MFA обеспечивает качественную аппаратную аутентификацию в веб-приложениях, позволяя полностью отказаться от паролей.

Но есть нюансы...

Проблема:
Ограниченная поддержка аппаратных средств аутентификаторов в прикладном ПО и сервисах

#1 Не все прикладное ПО и корпоративные сервисы (веб-порталы, CRM и ERP-системы, VDI и т.д.) поддерживают аппаратные устройства.

#2 Администраторы используют многофакторную аутентификацию выборочно, в зависимости от сервиса вместо единого цифрового удостоверения в виде токена или смарт-карты.

Решение

РУТОКЕН + AVANPOST

Нативная интеграция Рутокен и системы класса Identity and Access Management — Аванпост FAM позволяет аутентифицировать пользователя по аппаратному аутентификатору в большинство сервисов.

Аванпост FAM — инфраструктурная система для создания, хранения и управления идентификационными данными.

Avanpost Access Manager решение класса Enterprise IAM

Avanpost Access Manager — инновационный Identity Provider для всех задач идентификации, аутентификации и авторизации. Поддержка любых приложений, инфраструктур и федераций с гарантированной безопасностью и надежностью

Все виды десктопных и веб-приложений, мобильных приложений, сервисов и микросервисов.

Геораспределённые, гибридные и кластеризованные инфраструктуры, в том числе с поддержкой федераций удостоверений.

Максимальная гибкость и адаптивность процессов и политик идентификации, аутентификации и авторизации.

Поддержка всех элементов корпоративной инфраструктуры (VPN, VDI, RDP, SSH, рабочие станции под управлением Linux и Windows).

IAM Plaftorm: набор лицензий Avanpost Access Manager

FAM
FEDERATED ACCESS MANAGER

Адаптивный центр управления многофакторной аутентификацией в корпоративных приложениях с поддержкой мультидоменных инфраструктур и федерации удостоверений

ПРОЕКТ $$

КОРОБКА $$

MFA+

Система многофакторной аутентификации для корпоративных систем с поддержкой стандартных протоколов в on-premise

КОРОБКА $$

Unified SSO

Unified Single Sign-on. Прозрачная аутентификация за счёт использования агента между десктопом (Logon, Agent) и вебом, централизованное завершение сессии пользователя в APMe. Кросс-протокольная прозрачная аутентификация между OIDC, SAML

ПРОЕКТ $$

WSSO

Единая точка входа для веб-приложений, технологичных сервисов и API с большим количеством пользователей

Дополнительные опции расширения лицензий Avanpost Access Manager

Device Control	Контроль устройств. Сбор и анализ признаков внешних устройств и агентов на них, с которых выполняется аутентификация, запоминание пользователя, предотвращение компрометации.	**КОРОБКА $**
Location Control	Контроль геолокации. Анализ признаков подключения пользователя, для определения геолокации, в процессе аутентификации.	**КОРОБКА $/2**
Adaptive MFA	Возможность дополнить инструментами настройки адаптивного сценария MFA, использует контекст профиля, типа доступа пользователя, сессии, запроса. Динамическое/адаптивное определение сценариев аутентификации, конструктор политик, аналитические отчеты.	**КОРОБКА $$**

Компоненты комплексного решения по управлению аутентификацией

Серверные компоненты

Avanpost FAM Server — основной компонент системы аутентификации, обеспечивающий обработку запросов на аутентификацию, хранение данных системы, публикацию интеграционных интерфейсов (OIDC, SAML, RADIUS, grps), публикацию личного кабинета пользователя и административной консоли.

Avanpost FAM Mobile Services — компонент системы, обеспечивающий работу мобильного приложения Avanpost Authenticator.

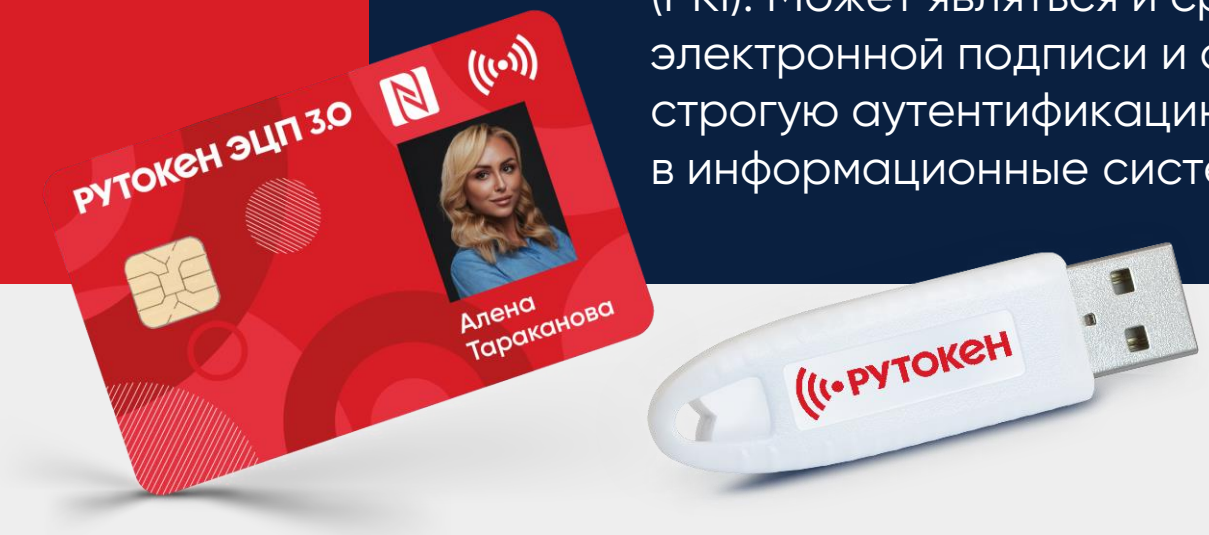
Компоненты комплексного решения по управлению аутентификацией

Программные клиентские компоненты

Avanpost FAM Agent — обеспечивает аутентификацию через Avanpost FAM в десктопных приложениях по технологии Enterprise SSO.

Аппаратные клиентские компоненты

Рутокен ЭЦП 3.0 — универсальный аутентификатор на основе технологии инфраструктуры открытых ключей (PKI). Может являться и средством электронной подписи и обеспечивать строгую аутентификацию в информационные системы.



Компоненты комплексного решения по управлению аутентификацией

Программные клиентские компоненты

Avanpost Windows/Linux Logon — обеспечивает аутентификацию через Avanpost FAM на рабочих станциях.

Аппаратные клиентские компоненты

Рутокен OTP — аппаратное средство для генерации криптографически вычисляемых одноразовых паролей (алгоритм TOTP) для усиленной аутентификации.

Компоненты комплексного решения по управлению аутентификацией

Программные клиентские компоненты

Avanpost Authenticator — мобильное приложение для аутентификации посредством push-запросов, запросов доступа без push, сканирования QR-кода, TOTP

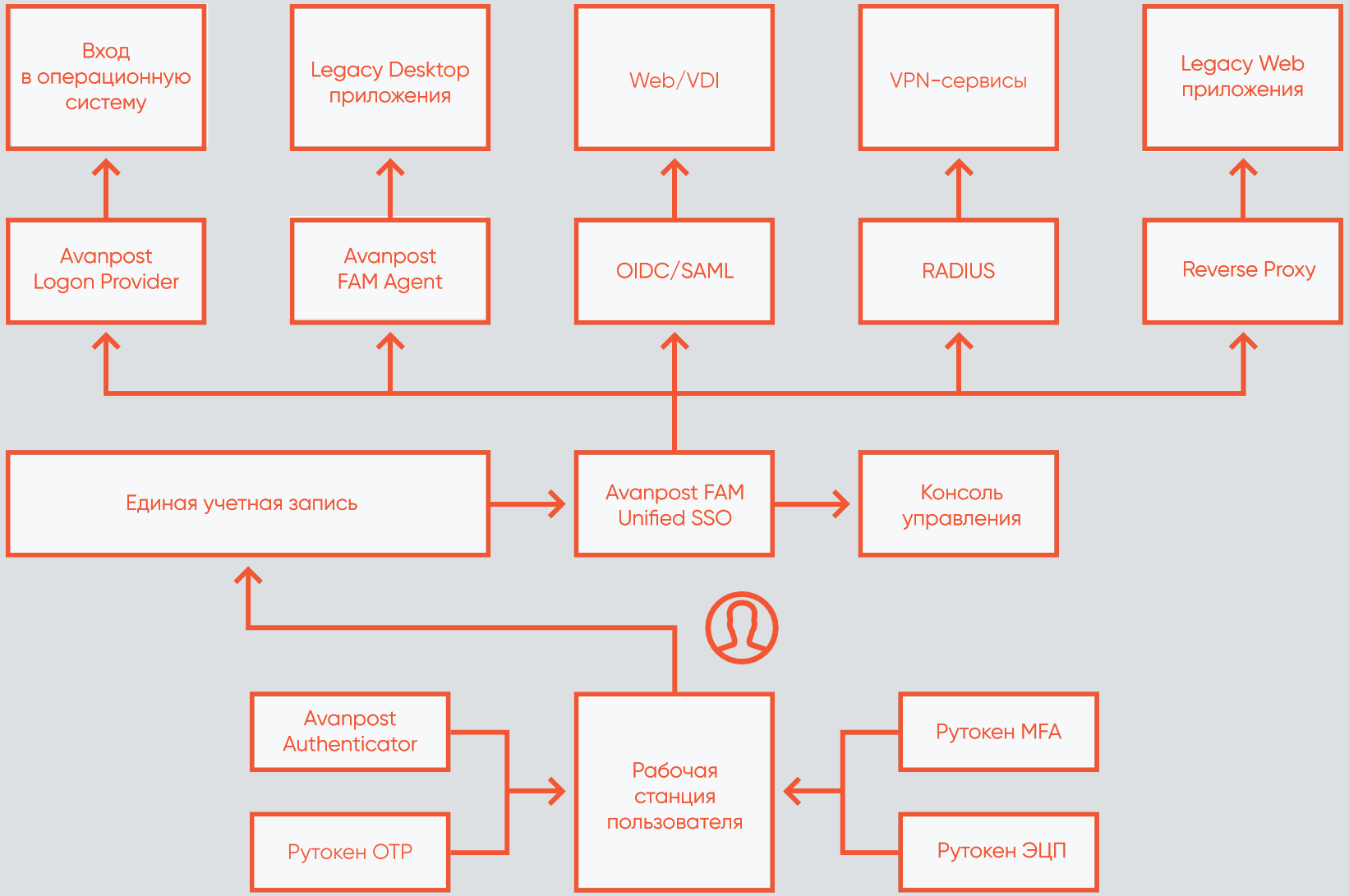
Аппаратные клиентские компоненты

Рутокен MFA — первый отечественный токен на базе технологии FIDO2, позволяющий полностью отказаться от паролей при работе в веб-приложениями, обеспечивая строгую аутентификацию.

Интеграция Avanpost Access Manager с прикладным ПО

Перечень стандартных протоколов плагинов	Комментарии	Область применения
Open ID Connect + OAuth 2.0 (OIDC)	Современный рекомендуемый способ аутентификации и авторизации, подходит для реализации SSO. Прикладное ПО, поддерживающее OIDC делегирует процесс проверки пользователя Identity Provider Avanpost.	Jira, Confluence, Git, Grafana) и отечественные (1С-Bitrix, корпоративные сервисы VK/Mail.ru, Яндекса и Т-Банка
SAML	Аутентификация в различных системах, преимущественно в web-приложениях. Более старый и менее гибкий аналог OIDC, но очень распространенный.	Atlassian, SAP, сервисы СберБизнес и 1С-Битрикс, офисный пакет Р7-Офис, семейство продуктов Citrix
RADIUS	Распространен в сетевом оборудовании, используется для аутентификации администраторов на маршрутизаторы\коммутаторы, удаленных пользователей при подключении по VPN и ряде VDI-систем.	В большинстве зарубежных (Cisco AnyConnect, Checkpoint Endpoint Security, Fortinet FortiClient); отечественных (Usergate Client, С-Терра Клиент, КриптоПро NGate Клиент) VPN-шлюзов и межсетевых экранов.
ADFS	Плагин применяется для нативной доменной аутентификации в бизнес-приложениях для Windows	Службы ADFS /Active Directory Federation Services
Reverse Proxy	Механизм для многофакторной аутентификации и SSO в веб-приложения. Компонент IAM-системы выступает в роли обратного http-proxy для всех сервисов, перехватывая штатные механизмы аутентификации.	Различные web-сервисы.
Logon Provider (Windows/Linux)	Механизм интеграции, обеспечивающий вход в учетные записи различных операционных систем. Реализуется через интерфейс Credential Provider в ОС Windows и PAM-модуля в ОС Linux.	Защита входа в локальную и доменную учетные записи, вход по протоколам удаленного доступа — RDP и SSH.

Кросс-протокольная аутентификация: Unified SSO



Avanpost FAM / Avanpost Unified SSO + Рутокен предоставляет комплексные сценарии управления доступом убирает интеграционные ограничения по работе прикладного ПО с аутентификаторами различных классов.

Кросс-протокольная аутентификация: Unified SSO

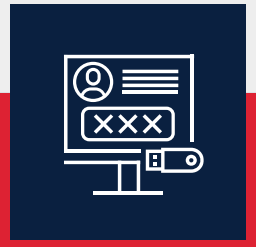
Преимущества:

Больше сценариев применения аппаратной аутентификации

за счет снятия технологических ограничений (PKI, Radius, FIDO)

Упрощение администрирования

за счет централизованного управления аппаратными аутентификаторами



Упрощение аутентификации для пользователей

за счет функции Unified SSO

КЕЙС 1. Многофакторная аутентификация для офисных и удаленных сотрудников

ЗАДАЧА

Обеспечить строгую многофакторную аутентификацию при помощи Рутокен ЭЦП в любых приложениях:

- Вход в **доменную учетную запись** ОС Astra Linux;
- **Домен** MS AD/Avanpost DS;
- Подключение удаленных сотрудников к **виртуальному рабочему столу** Termidesk VDI через **VPN** КриптоПро NGate;
- Возможность использовать **резервные механизмы** проверки аутентификации.

СОСТАВ РЕШЕНИЯ

- Avanpost FAM с компонентом Avanpost FAM Agent;
- Рутокен ЭЦП для каждого пользователя;
- Мобильное приложение Avanpost Authenticator на устройстве пользователя;
- УЦ для выпуска технологических сертификатов Avanpost CA.

КАК ЭТО РАБОТАЕТ

Avanpost FAM настраивается в режиме idP с существующими сервисами:

- **Logon Provider** для ОС Astra Linux;
- **OpenID Connect + oAuth 2.0** для Termidesk VDI;
- **RADIUS** для КриптоПро NGate.

КЕЙС 1. Многофакторная аутентификация для офисных и удаленных сотрудников: результат

Пользователь на рабочем месте или при удаленной работе использует устройство Рутокен ЭЦП для входа во все сервисы:

- входит в свою доменную учетную запись через токен на рабочем месте.

При удаленной работе пользователь проходит проверки:

- для запуска VPN-соединения нужно подключить Рутокен ЭЦП и ввести PIN-код;
- для подтверждения личности пользователю необходимо отправить Push-уведомление через приложение AvanPost или ввести одноразовый пароль в VPN-клиент.

Используя связку Рутокен ЭЦП и Avanpost FAM как удалённый, так и офисный сотрудник получают унифицированный сценарий аутентификации с прозрачным входом по технологии Unified SSO в рамках доверенного рабочего места:

- при аутентификации на АРМ сотрудника обеспечивается усиленная аутентификация через мобильное приложение Avanpost Authenticator или строгая аутентификация при помощи ЭП на Рутокен ЭЦП;
- после аутентификации на АРМ при подключении к VDI или VPN может быть реализован один из сценариев: Рутокен ЭЦП или Avanpost Authenticator;
- в соответствии с заданными администратором политиками механизма Unified SSO может быть пропущена проверка дополнительных аутентификаторов.

КЕЙС 2. Усиленная аутентификация по одноразовому паролю в различные корпоративные системы

ЗАДАЧА

Компания использует Рутокен OTP для доступа к своему частному облаку в Яндекс.Клауд. **Требуется расширить перечень используемых систем для уже приобретенных аутентификаторов.**

Для компании актуальны сервисы:

- ERP система 1С:Предприятие;
- База знаний на базе Atlassian Confluence;
- платформа ВКС TrueConf.

СОСТАВ РЕШЕНИЯ

- Avanpost FAM с компонентом Avanpost FAM Agent;
- Рутокен ОТП для каждого пользователя.

КАК ЭТО РАБОТАЕТ

Avanpost FAM выступает в качестве IdP-провайдера во всех сервисах, где реализована поддержка федеративной аутентификации по следующим протоколам:

- SAML для Яндекс.Клауд;
- OpenID Connect + oAuth 2.0 для тонкого/web-клиента 1С: Предприятие;
- Модуль Enterprise SSO через Avanpost FAM Agent для толстого клиента 1С: Предприятие;
- SAML или OpenID Connect для базы знаний Confluence;
- коннектор ADFS для ВКС TrueConf

КЕЙС 2. Усиленная аутентификация по одноразовому паролю в различные корпоративные системы: результат

Пользователь на рабочем месте или при удаленной работе использует устройство Рутокен ОТП для входа ВО ВСЕ СЕРВИСЫ:

Перенаправляется

в корпоративный IdP Avanpost FAM, где проверяется одноразовый код Рутокен ОТП и другой допустимый фактор

Открывает

толстый/тонкий/web-клиент 1С: Предприятие и за счет технологии Unified SSO проходит прозрачную аутентификацию без дополнительного запроса факторов, либо использует Рутокен ОТП (зависит от настроенного сценария)

Может проходить

прозрачную аутентификацию во все корпоративные приложения

КЕЙС 3. Беспарольная аутентификация в веб-сервисы с поддержкой SSO

ЗАДАЧА

Требуется обеспечить беспарольную аутентификацию при помощи Рутокен MFA в различные корпоративные сервисы и порталы.

СОСТАВ РЕШЕНИЯ

- Avanpost FAM с компонентом Avanpost FAM Agent;
- Компонент Reverse Proxy;
- Мобильное приложение Avanpost Authenticator на устройстве пользователя;
- Рутокен MFA на каждого пользователя.

КАК ЭТО РАБОТАЕТ

ПОЛЬЗОВАТЕЛЬ получает беспарольную аутентификацию во все используемые на предприятии веб-ресурсы

Avanpost FAM имеет в своем составе портал самообслуживания, который позволяет пользователю самостоятельно привязать свой аутентификатор к ресурсам.

ЗАКАЗЧИК получает современную беспарольную аутентификацию на веб-порталах, которые не имеют встроенной поддержки FIDO2

Avanpost FAM позволяет использовать современные FIDO2-аутентификаторы на ресурсах с поддержкой OIDC, SAML и для Legacy веб-приложений через механизм Reverse Proxy.

КЕЙС 4. Минимизация аутентификаций для пользователей в течение дня за счет Unified SSO

ЗАДАЧА

Обеспечить строгую многофакторную аутентификацию при помощи Рутокен ЭЦП с прозрачным последующим входом во все приложения: веб-портал, внешний шлюз, внутренний шлюз, независимо от формата работы (офис или удаленная работа).

СОСТАВ РЕШЕНИЯ

- Avanpost FAM с компонентом Avanpost FAM Agent;
- Модуль Unified Single-Sign-On для Avanpost FAM
- Рутокен ЭЦП для каждого пользователя;
- Мобильное приложение Avanpost Authenticator на устройстве пользователя.

КАК ЭТО РАБОТАЕТ

Технология Unified SSO вводит понятие «сессии пользователя» для всех возможных сценариев AvanPost FAM и является уникальной для российского рынка.

- Пользователь может зайти в любой сервис, используя компоненты Avanpost FAM Agent или AvanPost Authenticator, после чего у администратора появляется возможность прозрачно пускать пользователя во все доступные корпоративные сервисы.
- При необходимости получения доступа к наиболее критичным сервисам, система может запросить повторную аутентификацию.

КЕЙС 4. Минимизация аутентификаций для пользователей в течение дня за счет Unified SSO: результат

Существенно упрощение пользовательского опыта.

Нет необходимости заново аутентифицироваться в каждый новый корпоративный сервис.

Единое управление пользовательскими аутентификаторами.

Единое цифровое удостоверение пользователя.

Одно устройство Рутокен Рутокен позволяет войти во все в корпоративные сервисы.

Централизованное завершение пользовательских сессий.

Совместное применение технологии Unified SSO в Avanpost FAM и аутентификаторов Рутокен существенно улучшает опыт использования многофакторной аутентификации рядовыми сотрудниками, делая ее более простой, чем использование небезопасных паролей.

Компания «Актив»

guardant

РУТОКЕН

AKTIV. CONSULTING

30 лет на рынке информационной безопасности

Имеем все необходимые лицензии на разработку СКЗИ и СЗИ

Собственная испытательная лаборатория

Являемся членом АЗИ, РОСЭУ, ТК26, ТК362, РусКрипто, АПКИТ, АБИСС

Аванпост – экосистема программного обеспечения по управлению доступом. Построена на базе полностью собственного программного обеспечения, лучшего в своем классе, не зависящего от сторонних решений и open source компонентов

Команда Аванпост организует и использует процессы безопасной разработки программного обеспечения, опираясь на прогрессивный технологический стек, опыт анализа и реверс-инжиниринга систем безопасности, создает наиболее защищенные решения

Продукты разработаны для использования в высоконагруженных средах с применением технологий распределенных вычислений, кластеризации, балансировки нагрузки, автоматического масштабирования, шардинга и т.д.

Придерживаемся идеологии максимальной открытости и технологической совместимости с отечественным программным обеспечением, обеспечивая взаимодействие и работоспособность различных программных компонентов, объединяя их в единую платформу

Архитектура продуктов предполагает использование в отказоустойчивых георасределенных инфраструктурах: реализуем проекты, где продукты включены в Mission critical и Business critical контуры

Разработка ведется с помощью двух современных технологических стеков:
Postgre SQL/.Net Core/EF/Akka.Net/Angular – для продуктов со сложной бизнес-логикой;
GoLang /BadgerDB/GRPC/Vue.js – для высокопроизводительных сервисов

Российский вендор-новатор в области безопасности идентификационных данных

*развивает свою экспертизу с 2007 г.

AVANPOST
Системы аутентификации и управления доступом

Экосистема AVANPOST IAM для обеспечения целостного подхода к безопасности предприятия

AVANPOST

Комплекс продуктов для управления многофакторной аутентификацией в приложениях с поддержкой мультидоменных инфраструктур и федерации удостоверений

Автоматизация управления жизненным циклом учетных записей и правами доступа:

- управление доступом сотрудников;
- управление технологическими учетными записями;
- управление привилегированными и административными учетными записями

Решения для управления сложными, неоднородными, нагруженными инфраструктурами для бесшовной миграции с MS AD, управления ресурсами в период сосуществования с привычными сценариями для администраторов.

FAM

FEDERATED ACCESS MANAGER

MFA+

Многофакторная аутентификация в корпоративных системах

Risk based MFA
Device Control
Location Control

Unified SSO

Single Sign-on - безопасная аутентификация в нескольких сайтах и приложениях, используя один набор учетных данных

WSSO

Единая точка входа для web-приложений, технологичных сервисов и API

IDM

IDENTITY MANAGEMENT
Identity Governance & Administration (IGA)

Система управления учетными записями и доступом к корпоративным ресурсам предприятия.

DCAP (data-centric audit and protection) (IDM+/ Varonis)

PAM

PRIVILEGED ACCESS MANAGEMENT
контроль привилегированного доступа

Система организованно хранит, отслеживает, обнаруживает и предотвращает несанкционированный привилегированный доступ к критически важным ресурсам.

DS

DIRECTORY SERVICE

Полностью российская служба каталогов, предназначенная для замены MS AD и управления Linux инфраструктурами.

CA замена удостоверяющего центра MS CA + сценарии автоматического выпуска и обновления сертификатов, уникальные для Linux-инфраструктуры

PKI

PUBLIC-KEY INFRASTRUCTURE

Управление жизненным циклом объектов инфраструктуры открытых ключей из единого центра.

Контактная информация

Андрей Шпаков

Руководитель направления многофакторной аутентификации, Компания «Актив»

shpakov@rutoken.ru
info@rutoken.ru

www.rutoken.ru

+7 495 925-77-90
+7 916 518-70-26

РУТОКЕН

Дмитрий Грудинин

Руководитель по развитию продуктовой линейки аутентификации Avanpost FAM/MFA+, Avanpost

dgrudinin@avanpost.ru

www.avanpost.ru

+7 968 023-92-05

AVANPOST