

Решения Atos для обеспечения кибербезопасности современных организаций

Trusted partner for your **Digital Journey**

© Atos

Atos

Услуги по обеспечению кибербезопасности

3600 экспертов по всему миру

Из In Fidem:
+ 58 в Канаде

Северная
Америка

300

Из SEC Consult:
+ 139 в CE
+ 1 в NE
+ 52 в GM
+ 2 в US

Северная
Европа

1100

Центральная
Европа

700

B&PS Consulting:
+ 37 в Северной Европе
+ 15 в Южной Европе

Южная
Европа

500

Из Motiv:
+ 180 в NE

Из digital.security:
+ 219 в SE
+ 17 в NE

Из Paladion:
+ 663 в GM
+ 16 в US

1000
Растущие
рынки

Atos на рынке кибербезопасности

Признанный лидер ведущими агентствами

Gartner



Top 3
Managed
Security
Services
Worldwide
(based on 2019
revenues)

LEADER
MSS in
Western Europe

**MAJOR
PLAYER**
MSS Worldwide



imagine your future.*



LEADER
MSSIAM
in France
Germany
Switzerland
UK and US

FORRESTER



**STRONG
PERFORMER**
Managed
Security
Services
in Europe

3

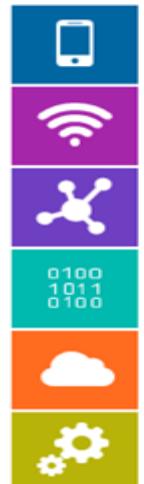


Top 2
IT Security
Services
Providers
in
EMEA
(based on
2019 revenues)



Богатый опыт внедрения

900+ заказчиков и 5 000 000+ конечных пользователей



End-to-end security

Финансы



Промышленность



Телеком / медиа



Здравоохранение



Реализованные в России проекты

В различных секторах экономики

DAIMLER



Проектирование,
внедрение средств
обеспечения ИБ McAfee

SIEMENS
Healthineers

Организация
удаленного управления
средствами
телемедицины

ALRUD

Проектирование
и внедрение MDM

РОСБАНК
SOCIETE GENERALE GROUP

Аудит группы
компаний по
внутреннему стандарту
ИБ «DARWIN»

SIEMENS

Разработка
процессов и ОРД
для использования
квалифицированной
ЭП в РФ



Единая карта
доступа сотрудника
ПАО «НЛМК»



НОРНИКЕЛЬ

Поставка и внедрение
Континент-АП



Разработка комплекта
ОРД для ЗПДн

Сертификаты и лицензии

Сертификаты:

- **ИСО 9001** Система менеджмента качества
- **ИСО 20000** Система менеджмента ИТ-сервисов
- **ИСО 27001** Система менеджмента информационной безопасности
- **ИСО 14001** Система экологического менеджмента
- Свидетельство о разрешении на работу с саморегулируемой организацией (**SRO**) № 092-77- 002-01-8

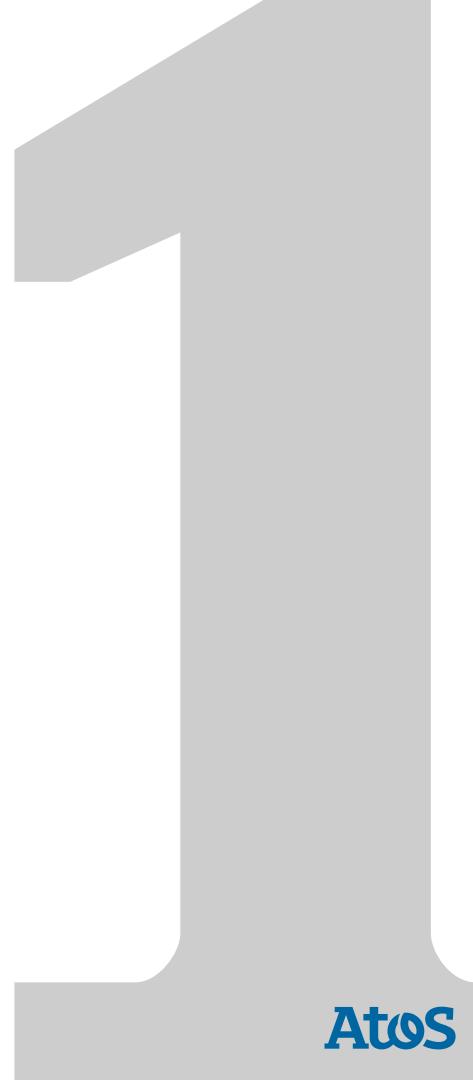


Лицензии:

- На осуществление разработки, производства, распространения, технического обслуживания шифровальных (криптографических) средств (**ФСБ № 6436**)
- На деятельность по разработке и производству средств защиты конфиденциальной информации (**ФСТЭК № 4521**)
- На деятельность по технической защите конфиденциальной информации (**ФСТЭК № 4522**)
- Услуги связи по передаче данных, за исключением услуг связи по передаче данных для целей передачи голосовой информации (**лицензия №103612**)
- Телематические услуги связи (**лицензия №103613**)
- Услуги связи по передаче данных для целей передачи голосовой информации (**лицензия №103614**)

Evidian

Решения
для многофакторной
аутентификации



Atos



Для каких задач?

- Безопасный быстрый доступ к ресурсам с технологией единого доступа с рабочих станций, планшетов и мобильных телефонов
- Внедрение многофакторной авторизации в приложениях и веб-ресурсах
- Сбор и аналитика подозрительной активности
- Реализация модели управления доступом на основе ролей



Почему Atos?

- Модульность
- Совместимость с любыми средами заказчика
- Возможность развертывания в облаке
- Отказоустойчивость

User Name	Display Name	Email	Unlocked/Locked	Actions
ragot96	Scholastique RAGOT	scholastique.ragot_96@idaae.net		
piermon92	Hildebert PIERRON	hildebert.pierron_92@idaae.net		
pasquea95	Ancelin PASQUER	ancelin.pasquier_95@idaae.net		
marchal100	Amélieane MARCHAL	ameliane.marchal_100@idaae.net		
marcel98	Robert MARCEL	robert.marcel_98@idaae.net		
gouplin97	Nicolas GOUPIL	nicolas.gouplin_97@idaae.net		
boutetm99	Marius BOUTET	marius.boutet_99@idaae.net		
bellec91	Claire BELLEC	claire.bellec_91@idaae.net		

Evidian

Enterprise Access Management



Enterprise SSO

Безопасный и быстрый доступ к программам и корп. ресурсам с технологией единого доступа с любых устройств



Authentication Manager

Многофакторная авторизация на стартовом экране ПК с поддержкой многопользовательского режима



SSPR

Сервис для самостоятельного восстановления паролей

Web Access Management



Web Access Manager

Многофакторная авторизация к SaaS-приложениям и корпоративным порталам

Identity Governance and administration

Автоматизация управления идентификационными данными, включая интеграцию с инструментами HR. Реализация ролевой модели управления доступом, синхронизация и управление учетными записями и паролями различных систем

Analytics and Intelligence

Подробная аналитика рисков

Выявление и отслеживание подозрительных действий, контроль использования приложений

Конкурентный анализ

	Avanpost	Indeed	RSA	One Identity	Evidian
AIM	Да	Да	Да	Да	Да
SSO	Да	Да	Да	Да	Да
WAM	Нет	Нет	Да	Да	Да
IGA	Нет	Нет	Да	Да	Да
Преимущества	Да	Нет	Да	Да	Да
Возможность работы в оффлайне			Нет	Нет	Да
Быстрое переключение между рабочими станциями			Нет	Нет	Да
Поддержка мобильных устройств			Да	Нет	Да
Средства аутентификации		PKI-карта и USB-токен	PKI-карта	PKI-карта, одноразовый пароль, биометрия, браслет, QR-код	

Enterprise Access Management

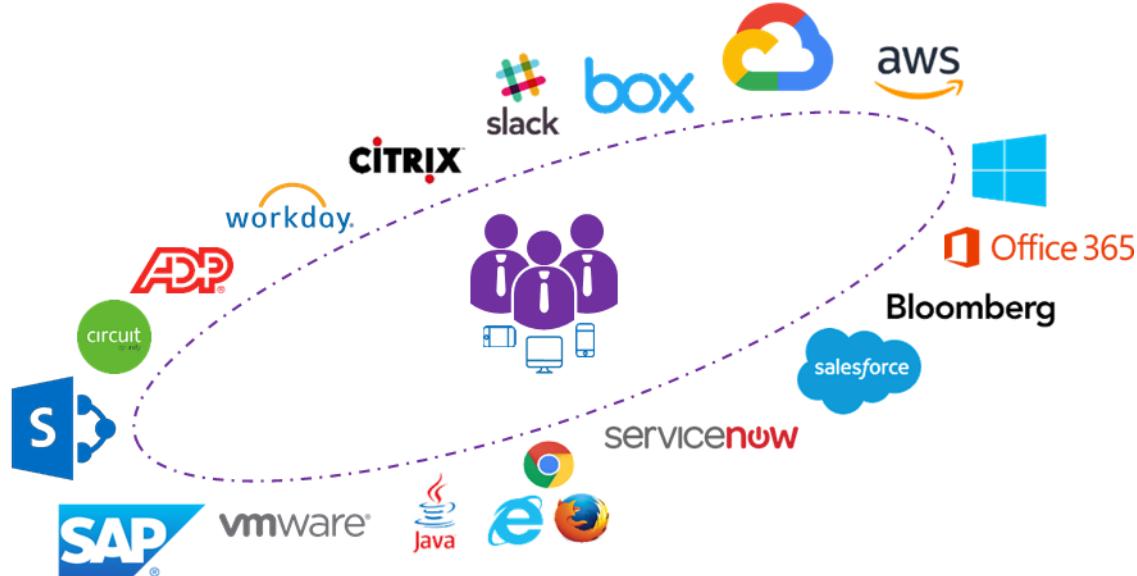
Authentication Manager



Application Access Management

Приложения являются основными компонентами бизнеса организации.

- ⚠ Некоторые из них являются критичными для работоспособности бизнеса и требуют повышенной безопасности, а также возможности доступа в любое время, в любом месте и с любого устройства



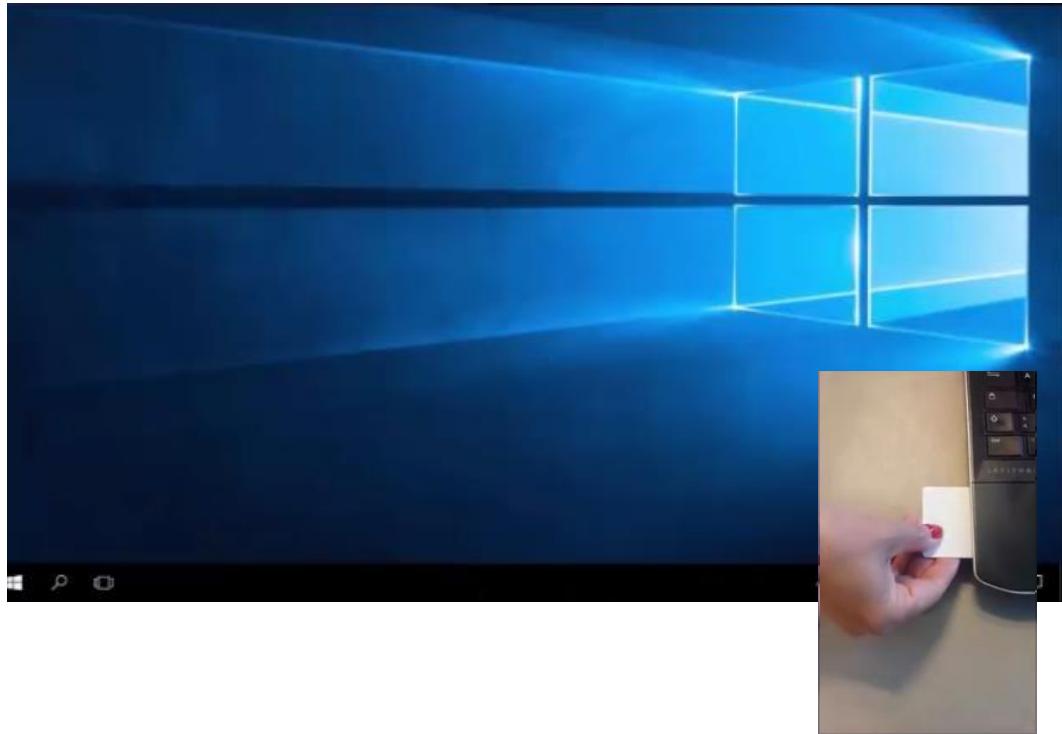
Authentication Manager

Авторизация с использованием Smart Card



Безопасный доступ к корпоративным ПК и серверам с помощью Authentication Manager:

- ▶ Поддержка большого списка способов авторизации
- ▶ Организация многопользовательского доступа (без переключения сессии Windows)
- ▶ Многофакторная авторизация
- ▶ Делегирование полномочий (например, уход сотрудника в отпуск)
- ▶ Журнал всех событий
- ▶ Авторизация онлайн или офлайн



Authentication Manager

Использование различных биометрических данных



Варианты хранения данных

- **Локально на рабочей станции**

Пользователи должны зарегистрировать свои биометрические данные на всех рабочих станциях, которые они будут использовать

- **На выделенной смарт-карте**

Пользователи вставляют свои смарт-карты, а затем сканируют свои биометрические данные

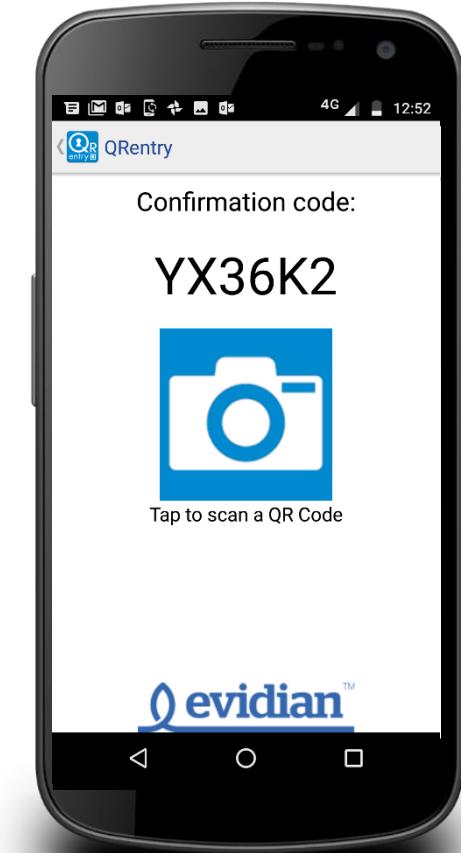
- **Внутри каталога LDAP**

Пользователи должны только сканировать свои биометрические данные



Authentication Manager - Qrentry

Неважно, подключен ли Ваш ПК или смартфон к сети

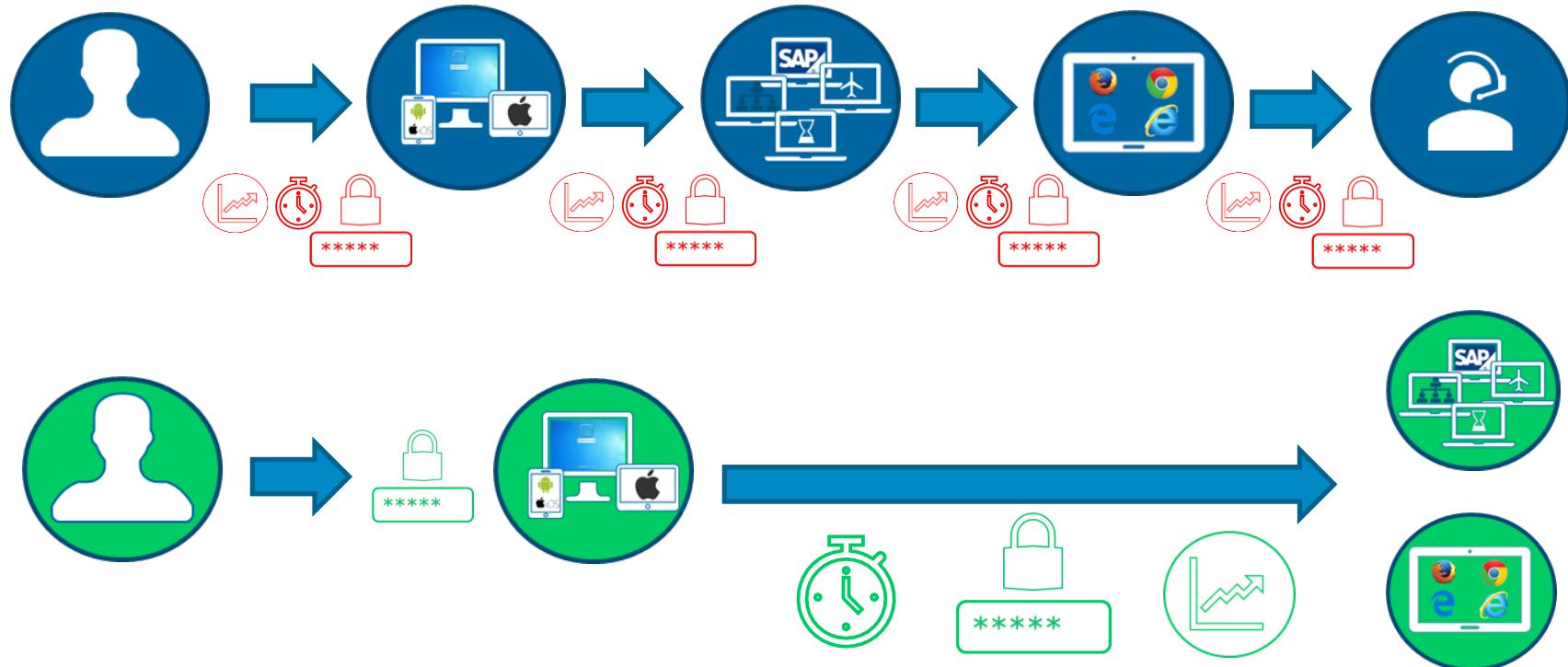


Enterprise Access Management

E-SSO

Типичный рабочий день с SSO и без него

Преимущество для любой организации



Свобода пользователей от запоминания и ввода паролей

Реализация ролевой модели управления доступом

- Внедрение сложных политик безопасности
- Пароли больше не принадлежат пользователю



Без использования Enterprise SSO	
Application	Password
Internet web	access
Mail	jeanne74
SAP	jeanne74
Intranet	jeanne1974
Web site	jeanne74

Решения Evidian:

- Устраняет очевидные пароли
- Применяют сложные политики паролей
- Производят регулярную смену пароля
- Гарантируют уникальность паролей
- Применяют метод аддитивной аутентификации

При использовании Enterprise SSO и применения политик безопасности

Application	Password
Internet web	F5?-xx80Hd2
Mail	iu(28~/&17Sq
SAP	67-#?p8x6sfA
Intranet	Tt6-(@2lkZ=a
Web site	;/lu6h-h2A*j

Простота использования

- Позволяет пользователям добавлять и регистрировать доп. приложения
- Далее происходит автозаполнение
- Обнаружение и заполнение абсолютно ненавязчиво, модификации приложений не требуются

Распознавание различных форм

- Запрос пароля
- Неправильный пароль
- Новый пароль
- Подтверждение

Взаимодействует с приложениями:



Enterprise Access Management

Self-service password request

Восстановление пароля

Восстановление пароля

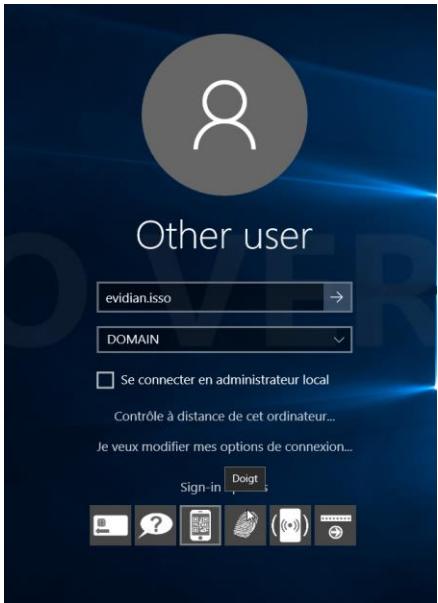
- Пользователи могут самостоятельно восстановить забытый пароль или PIN-код с экрана входа в систему или с портала управления корпоративным доступом:
 - Отвечая на вопросы безопасности
 - Используя ОТР
 - Используя свой смартфон с QRentry
 - С помощью Push-уведомления
 - Через портал управления корпоративным доступом
- Сброс можно выполнить, даже если рабочая станция не подключена, и без вмешательства службы поддержки



Оповещения на телефон



С рабочей станции



С веб-портала

The screenshot shows a "SMS OTP PASSWORD RESET" page. It displays a confirmation message: "Confirmation code sent to: 0677777777. Confirmation code is valid for 04:56." Below this, instructions say "Please fill-in the Confirmation Code you have received" followed by a "Confirmation Code" input field. Further down, there are fields for "Enter your new password here" (labeled "New password") and "Confirm new password", both with their respective input fields. At the bottom are "Submit" and "Clear" buttons.

ENTERPRISE ACCESS MANAGEMENT 10.00 b6500

Web Access Management



Web Access Management

Управление доступом к веб-приложениям



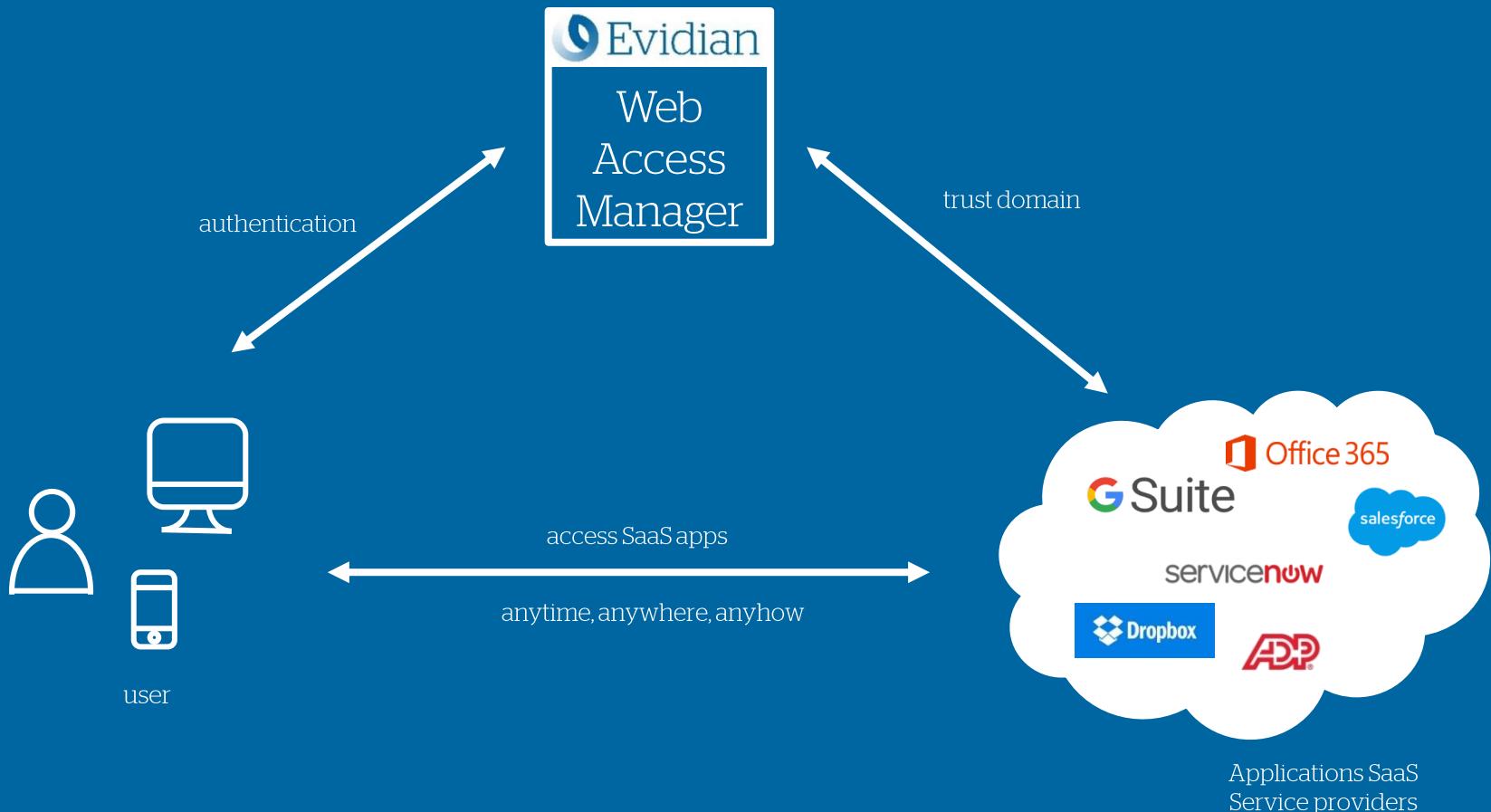
Пользователи могут получить безопасный доступ ко всем SaaS-приложениям, размещенным в облаке и корпоративным ресурсам, с помощью единой аутентификации

Преимущества:

- ▶ Простота использования - вход в систему / аутентификация требуется только один раз
- ▶ Минимизация обращений в техническую поддержку
- ▶ Строгая аутентификация

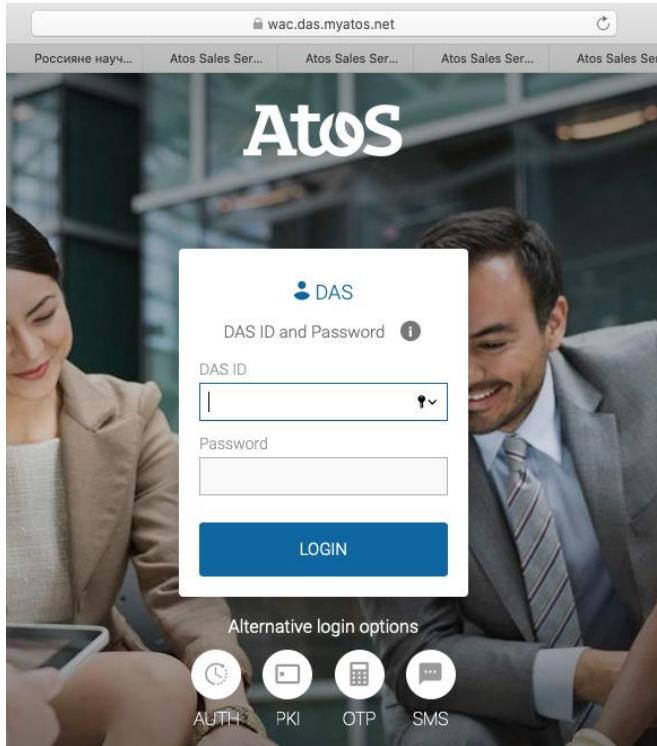
Еще больше повышает безопасность благодаря контекстной аутентификации: в зависимости от их местоположения, среды просмотра, времени и ресурса, к которому они пытаются получить доступ

Evidian WAM



Evidian Web Access Manager

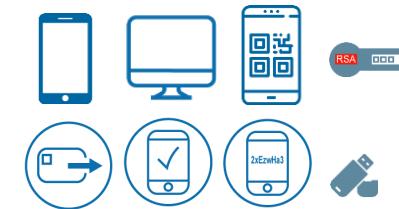
Безопасный доступ к вашим веб-ресурсам



Доступные способы авторизации:

- Логин/пароль
- Smart card
- SMS OTP
- e-mail OTP
- Push уведомления
- QRentry
- Сертификаты
- Социальные сети

и другие



Все эти способы могут быть использованы
для многофакторной авторизации

Основные преимущества

Enterprise Access Management



Безопасность

- ▶ Доступ к приложениям и ресурсам с помощью MFA
- ▶ Использование строгих политик безопасности



Продуктивность

- ▶ Сокращение времени простоя из-за заблокированных учетных записей
- ▶ Частый ввод сложных паролей - потеря производительности



Удобство

- ▶ Аутентификация из любого места на любом устройстве
- ▶ Избавление от необходимости запоминать и вводить пароли



Соответствие

- ▶ HIPAA, CFR21 Part11, PSD2, HAS...
- ▶ Соответствие законам о персональных данных

Identity Governance & Administration



Identity Governance & Administration

Инструмент регулирования доступа к приложениям



Только конкретные сотрудники с необходимым набором прав имеют доступ к конкретным ресурсам



Организации должны иметь возможность:

- ▶ Расширить возможности управления правами конечных пользователей
- ▶ Ускорить доступ к приложениям и ресурсам, увеличив производительность и удовлетворенность пользователей
- ▶ Сфокусироваться на мониторинге и снижении рисков компании, не создавая утомительных процессов для ответственных лиц
- ▶ Обеспечить применение политик безопасности и выявлять несоответствия
- ▶ Разрешить пользователям запрашивать права доступа и восстанавливать свои пароли

Identity Governance & Administration

Преимущества



Автоматизация

- ▶ Управление аккаунтами сотрудников, партнеров, клиентов
- ▶ Права доступа на основе ролей



Безопасность

- ▶ Мониторинг и снижение рисков, связанных с правами пользователей



Продуктивность

- ▶ Управление доступом сотрудников, партнеров и клиентов к ресурсам и приложениям



Отчеты и соответствие

- ▶ Инструменты аудита и подробная отчетность
- ▶ Соответствие законам о персональных данных

Evidian Analytics & Intelligence

Evidian A&I включает широкий набор отчетов

Визуализация данных и тренды



- Аутентификации пользователей
- Риск аутентификации для пользователей
- Пользователи
- Доступ к приложениям
- Пользователи с нарушениями SoD
- Пользователи без прав
- Запросы о назначении / отзыве прав
- Жизненный цикл пользователя
- Смена пароля
- Сбои инициализации
- Регистрация / отмена регистрации пользователя для услуги

Analytics & Intelligence

Преимущества

Выявление рисков

- Выделение ключевых индикаторов риска (KRI) и мониторинг действий, которые считаются подозрительными, независимо от того, были ли они выполнены пользователем или администратором

Сокращение затрат

- Учетные записи для облачных приложений создаются автоматически после запроса пользователя и предоставления администратором доступа.
- Возможности отслеживания полноты использования запрошенных доступов и сокращения издержек



Аппаратные решения безопасности

HSM и решения обеспечения
безопасности VPN-сетей



Аппаратные решения безопасности

HSM и решения обеспечения безопасности
VPN-сетей



Для каких задач?

- Безопасность транзакций и других процессов в финансовом секторе
- Целостность и безопасность криптографических операций
- Организация безопасного обмена данных в корпоративной сети



Преимущества Atos

- Высочайшая степень защиты и безопасность
- Сертифицированные решения
- Собственные центры разработки ПО
- Широкая линейка оборудования под любые задачи заказчика
- Высокие показатели производительности



Решения для высоких нагрузок

Worldline Adyton и Trustway Crypt2pay

Worldline Adyton



Crypt-2-Pay



HSM + приложения = безопасность в едином корпусе!

Примеры применения HSM

HSM имеют широкое применение во всех сферах деятельности:

- ▶ Для шифрования баз данных
- ▶ Для электронного документооборота (для безопасного хранения и использования ключей электронных подписей)
- ▶ Для безопасного хранения данных в облачных хранилищах
- ▶ Для защиты передачи данных с IoT устройств
- ▶ Для защиты от несанкционированного производства продукции и подделки
- ▶ Для предотвращения атак на IoT устройства (при подключении злоумышленников к производственным сетям и изменения количества, характера или качества производимой продукции)

и множество других примеров





HSM-модуль



Максимальная безопасность

- Обнаружение и реагирование на вмешательства (обнуление ключей)
- Сертификация безопасности FIPS 140-2, CB, PCI HSM



Максимальная надёжность

- Долгий жизненный цикл
- Двойные блоки питания с возможностью замены «на горячую»



Высочайшая производительность

- **7000 TPS** асимметричные ключи
- **10 000 TPS** симметричные ключи



Удобный для пользования дизайн

- Встроенные пользовательские интерфейсы
- Дополнительное устройства управления не требуется



Кастомизированное решение

- Индивидуальные решения в рамках ПО модулей HSM
- Возможность удаленного управления

Готов ответить на Ваши вопросы

Артем Иванов

M +7 960 116 06 23

artem.ivanov@atos.net



@AtosServers

Atos