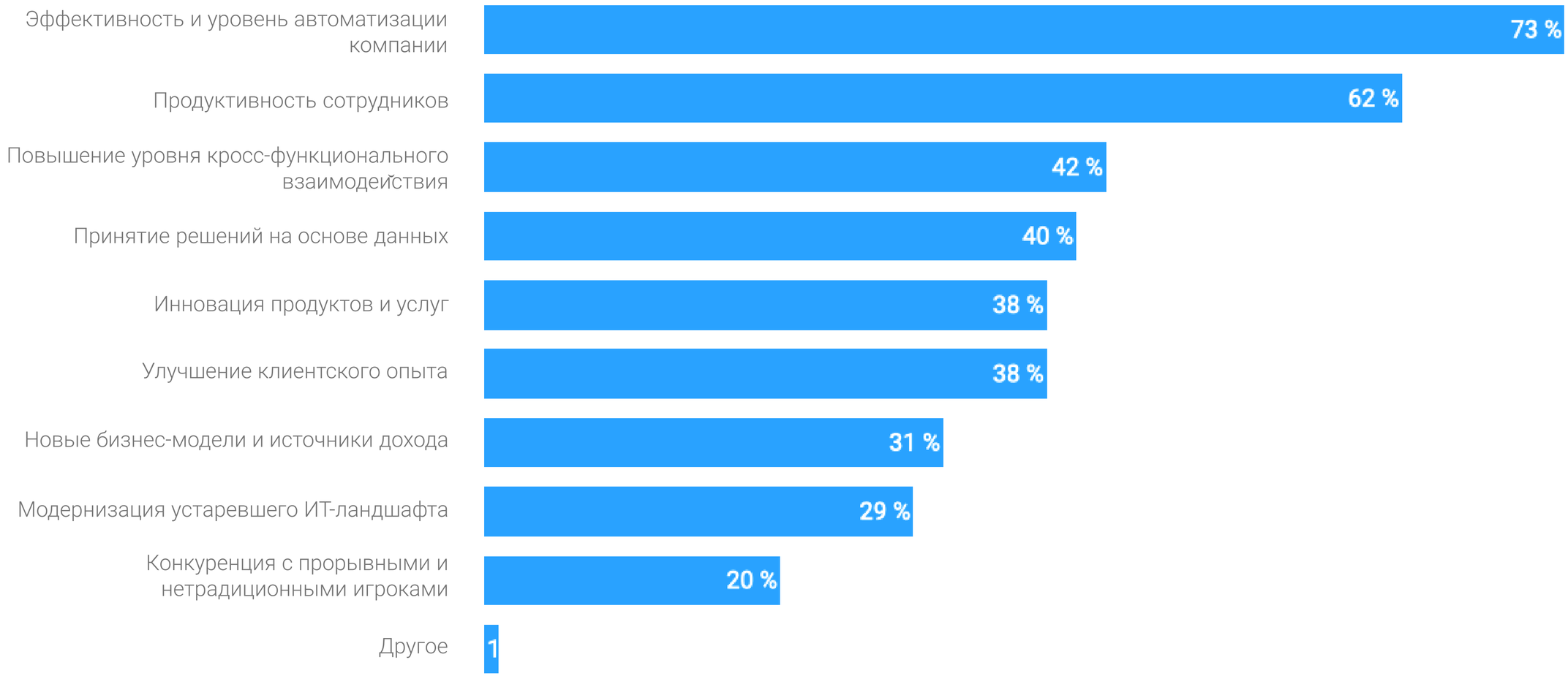
Что отечественные enterprise mobility management платформы могут предложить банковскому сектору в современных условиях

ОТКРЫТАЯ МОБИЛЬНАЯ ПЛАТФОРМА

Какую задачу трансформации обеспечивает корпоративная мобильность?



ГОСТ Р 57580.1

Национальный Стандарт РФ «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер»

Базовый состав мер по защите информации от раскрытия и модификации при осуществлении удаленного доступа

Предоставление удаленного доступа только с использованием мобильных (переносных) устройств доступа, находящихся под контролем системы централизованного управления и мониторинга (системы Mobile Device Management, MDM).

Базовый состав мер по защите информации от раскрытия и модификации при ее обработке и хранении на мобильных (переносных) устройствах

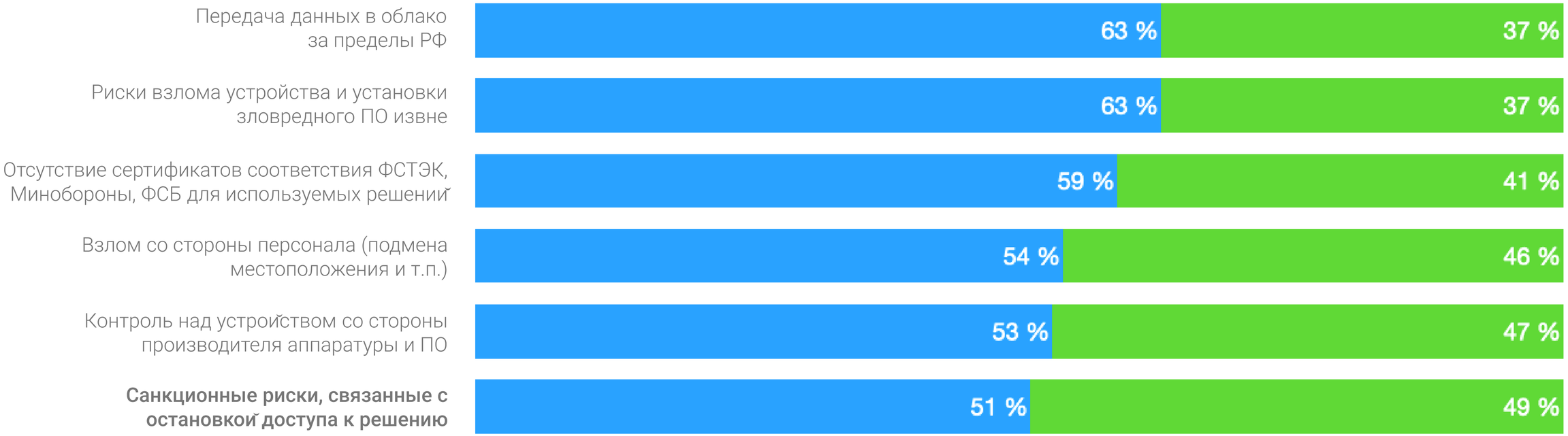
Применение системы централизованного управления и мониторинга (MDM-системы), реализующей:

- шифрование и возможность удаленного удаления информации, полученной в результате взаимодействия с информационными ресурсами финансовой организации; аутентификацию пользователей на устройстве доступа;
- блокировку устройства по истечении определенного промежутка времени неактивности пользователя, требующую выполнения повторной аутен тификации пользователя на устройстве доступа;
- управление обновлениями системного ПО устройств доступа;
- управление параметрами настроек безопасности системного ПО устройств доступа;
- управление составом и обновлениями прикладного ПО;
- невозможность использования мобильного (переносного) устройства в режиме USB-накопителя, а также в режиме отладки;
- управление ключевой информацией, используемой для организации за щищенного сетевого взаимодействия;
- возможность определения местонахождения устройства доступа;
- регистрацию смены SIM-карты;
- запрет переноса информации в облачные хранилища данных, расположенные в общедоступных сетях (например, iCloud);
- обеспечение возможности централизованного управления и мониторинга при смене SIM-карты.

Разработан Центральным банком Российской Федерации и Научно-производственной фирмой «Кристалл».
Утвержден и введен в действие 8 августа 2017 г. N 822-ст Приказом Федерального агентства по техническому регулированию и метрологии

Стоп-факторы, препятствующие внедрению или развитию решений корпоративной мобильности

Риски требуют глубокой переоценки. Ландшафт пригодных решений - пересмотра.



Открытая мобильная платформа

ОС Аврора

Единственная мобильная ОС в реестре российского ПО, сертифицирована ФСТЭК и ФСБ.

Аврора Центр

Платформа управления корпоративными мобильными устройствами и приложениями. Включена в реестр российского ПО и сертифицирована ФСТЭК России.

Аврора TEE

Среда исполнения для операций, требующих максимального доверия и надёжности — аутентификации пользователя, хранения ключевой информации, выполнения криптографических операций и контроля функционирования ОС Аврора.

СледопытSSL

Программное средства криптографической защиты информации Предназначено для зашиты конфиденциальных данных при их обработке, хранении и передаче по открытым каналам. Соответствует требованиям ФСБ России к СКЗИ класса КС2

СледопытVPN

Для обеспечения доверенного канала данных между мобильным устройством и корпоративной инфраструктурой. Для защиты передаваемых данных используются отечественные алгоритмы ГОСТ.Р 34.10-2012, ГОСТ.Р 34.11-2012 и ГОСТ.Р 34.12-2015.

Внедрения

ВСЕРОССИЙСКАЯ ПЕРЕПИСЬ НАСЕЛЕНИЯ 2022

Планшеты для переписчиков

360 тыс. устройств

Ростелеком

Цифровой монтажник связного оборудования

1,5 тыс. устройств

ПОЧТА РОССИИ

Цифровой почтальон

15 тыс. устройств

РЖД Российские железные дороги

Эксплуатация инфраструктуры

3,6 тыс. устройств

ИНТЕР РАО

Контроль исполнения
осмотров и обслуживания

РОСАТОМ

Доверенная мобильная среда

Аврора Центр

Ключевые возможности

- активация устройств и ввод в эксплуатацию;
- управление состоянием и поведением устройств;
- управление пользователями и доступом;
- доставка приложений на устройства;
- обновление ПО на устройстве;
- инвентаризация устройств и мониторинг событий.

Инструменты

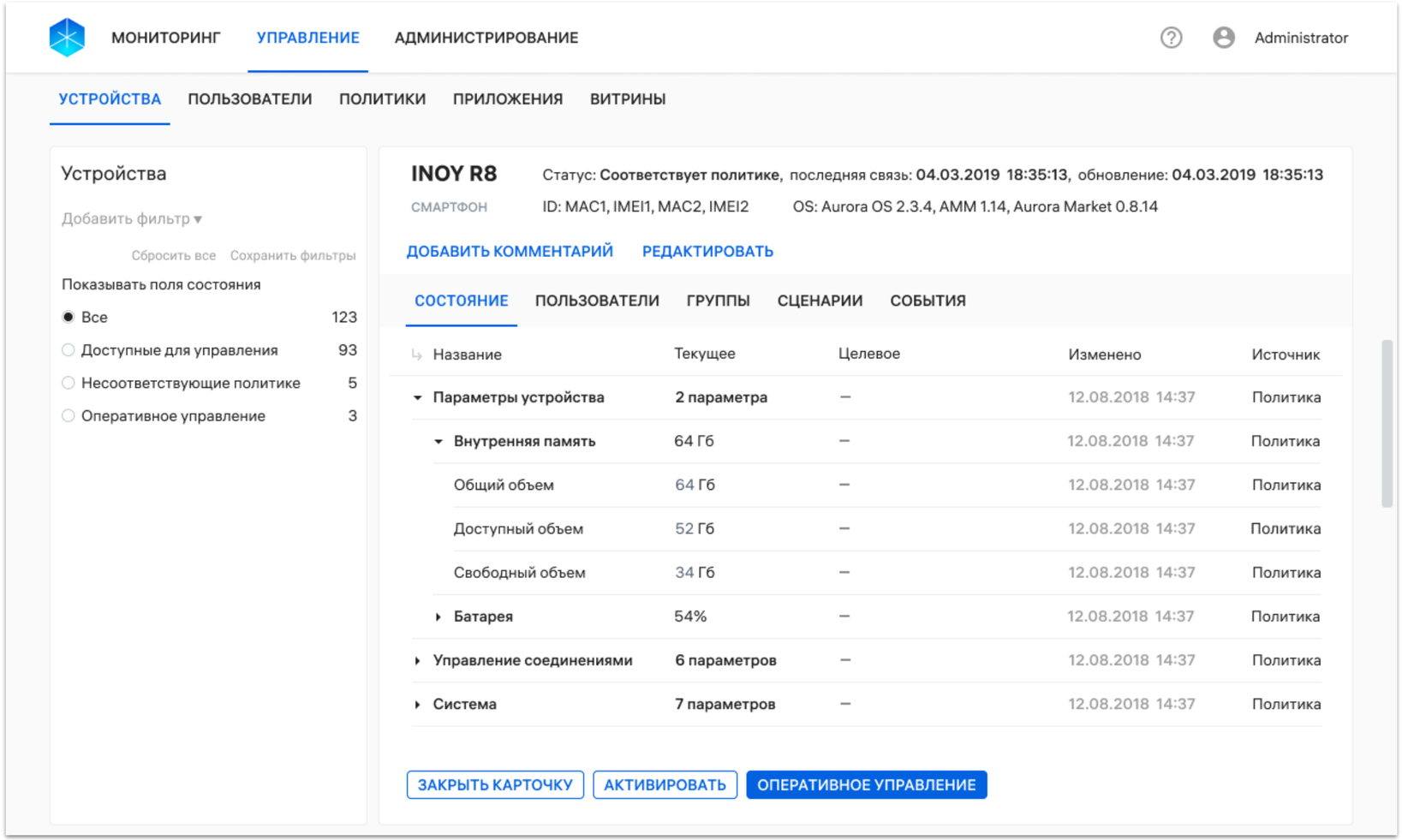
- Прямые оперативные команды;
- Массовые операции:
  - Политики;
  - Офлайн сценарии.

Механизмы

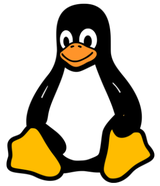
- Push;
- Multitenancy.

Характеристики

- On-premise deployment;
- Поддержка до 550k устройств.



Аврора Центр расширяет поддержку операционных систем



Функциональные блоки Аврора Центр принципиально позволяют управлять любыми устройствами

Identity management (IDM)

- Факторы
- Технологии

- Пароли: HMAC & OTP/TOTP/HOTP
- Сертификаты SSL Client Certificate, ГОСТ ЭП
- Mutual TLS
- Аппаратные токены: ruToken, eToken, ESMART
- Доменная аутент-ия SPNEGO/Kerberos
- LDAP аутентификация
- Биометрия

———

- OpenID/OAuth 2.0/SAML
- ESSO/Enterprise SSO
- RADIUS
- MS Credential Provider
- PAM Linux

Rule Engine & Event Classification (Core)

- Политики
- Сценарии
- Команды
- События

- Deployment Rules
- Permissions Rules
- Configurations Rules
- Необратимые операции

———

- State
- Event logs

Repositories (Маркет)

- Сборки

- Firmware
- OS
- App
- Patch
- Drivers

Управление идентификацией и доступом

Управление состоянием и поведением

Мониторинг состояния и активности

Управление доставкой и развертыванием ПО

Программные компоненты

Системное ПО

- Firmware
- ОС
- Системные приложения

Прикладное ПО

- Служебное ПО
- Пользоват, приложения

Аппаратные компоненты

- Процессоры
- Чипы-интерпрет.
- Контроллеры
- LTE
- WLAN
- Модули провод. связи
- Модули питания
- Батареи
- Считывател.
- Сенсоры
- GPS
- GLONASS
- Камеры

Оконечные устройства

Firmware based device

- Датчики геопозиц.
- 3D аксел-метры.
- Датчики (темп, освещен. движен.)
- Считывател (отпечатки, RFID и т.д.)
- Контрол-ры исп. механизмов
- Контрол-ры доступа
- Модули ввода-вывода
- Сетевые (IP) камеры
- Носимые/автомобильные камеры
- Модули распозн. лиц

OS based device

Стационарные персонального пользования

- Desktop

Носимые персонального пользования

- Смартфоны и планшеты
- Ноутбуки
- Терминалы сбора данных
- POS терминалы
- Кассовые системы

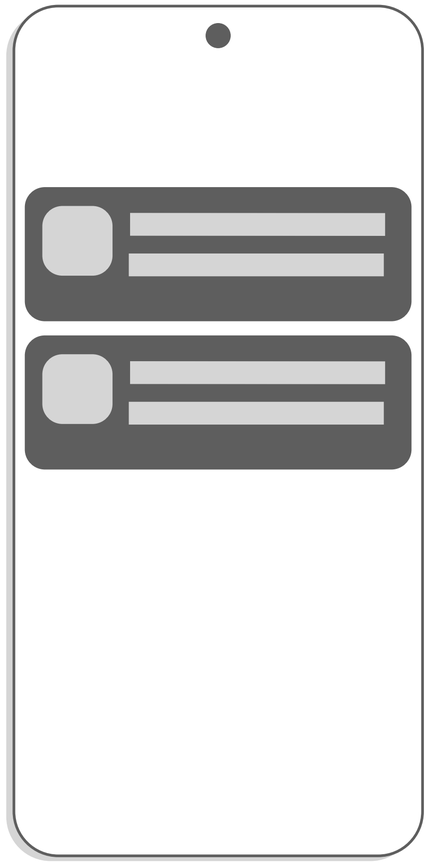
Стационарные общего пользования

- Киоски
- Терминалы доступа
- Электронные консъержи

Стационарные общего пользования без непосредственного взаимодействия с пользователем

- Телевизоры и панели

Аврора Центр развивает собственную инфраструктуру транспорта



Push сервис, разработанный нами в развитие экосистемы Аврора, мы готовы предлагать как самостоятельный продукт, например для доставки команд и сообщений для устройств на ОС Android в режиме реального времени.

Аврора Центр нацелена стать ядром для развития вертикальных кейсов

Perceptions & Network Layer

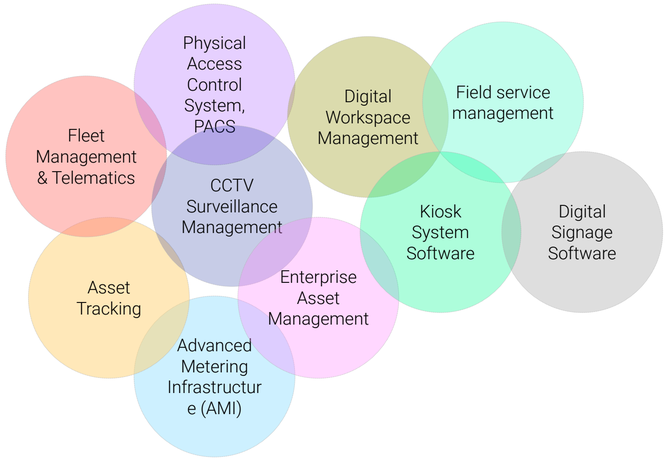
Подключенные устройства различных типов, форм-факторов, различных операционных систем и без операционных систем

Processing Layer

- Identity & Access Management
- Device lifecycle management (DLM)
- Event logging
- Rule Engine
- Event Classification
- Usage Management
- App Distribution
- Inventory Management
- Data governance

Core-функционал Аврора Центр: Rule Engine, App distribution, Event logging

Application Layer

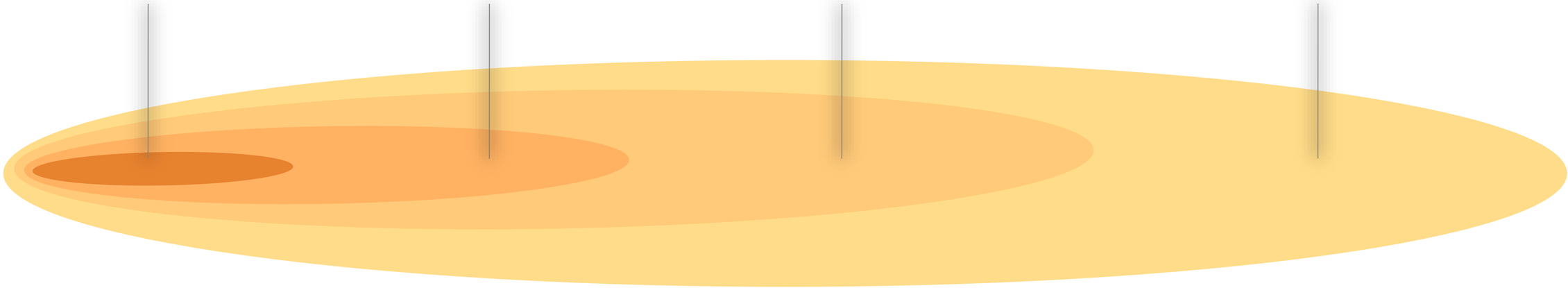


Вертикальные бизнес-решения, создаваемые партнерами на базе Аврора Центр

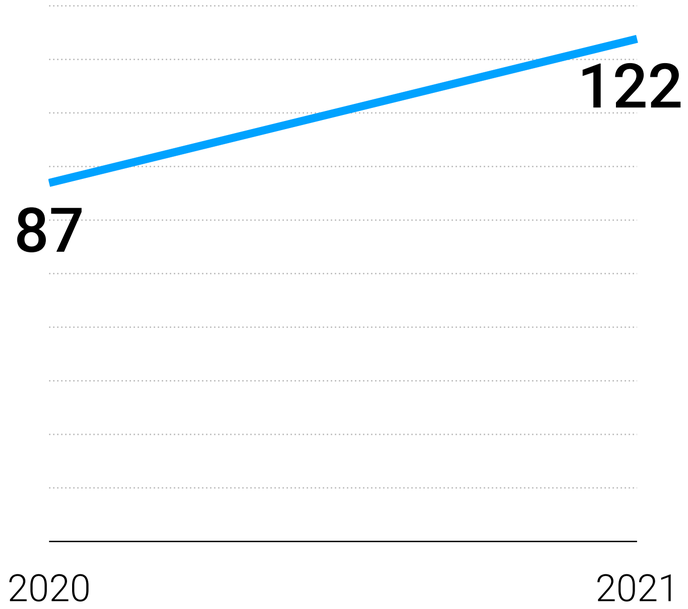
Business Layer

- ITSM & Order Management
- Управление телекоммуникационными расходами
  Telecom Expense Management (TEM)
- Управление закупкой
  Device procurement

Глубокая интеграция в бизнес процессы управления процессами и инфраструктурой у конечных бизнес-пользователей (выбора поставщиков и заключения контрактов на связь и устройства)



ОМП активно развивает партнерство с производителями устройств, разработчиками ПО и интеграторами



Клуб пользователей российских корпоративных мобильных технологий

https://кормтех.рф

Производители интегральных микросхем, смартфонов, планшетных компьютеров, систем видеонаблюдения, контроля и управления доступом.

Партнеры - разработчики ПО

Заказчики и эксплуатанты, производители устройств и разработчики ПО.

Спасибо!

Герман Чеботарев
g.chebotarev@omp.ru