Программно-определяемая инфраструктура как инструмент повышения киберустойчивости финансовой организации

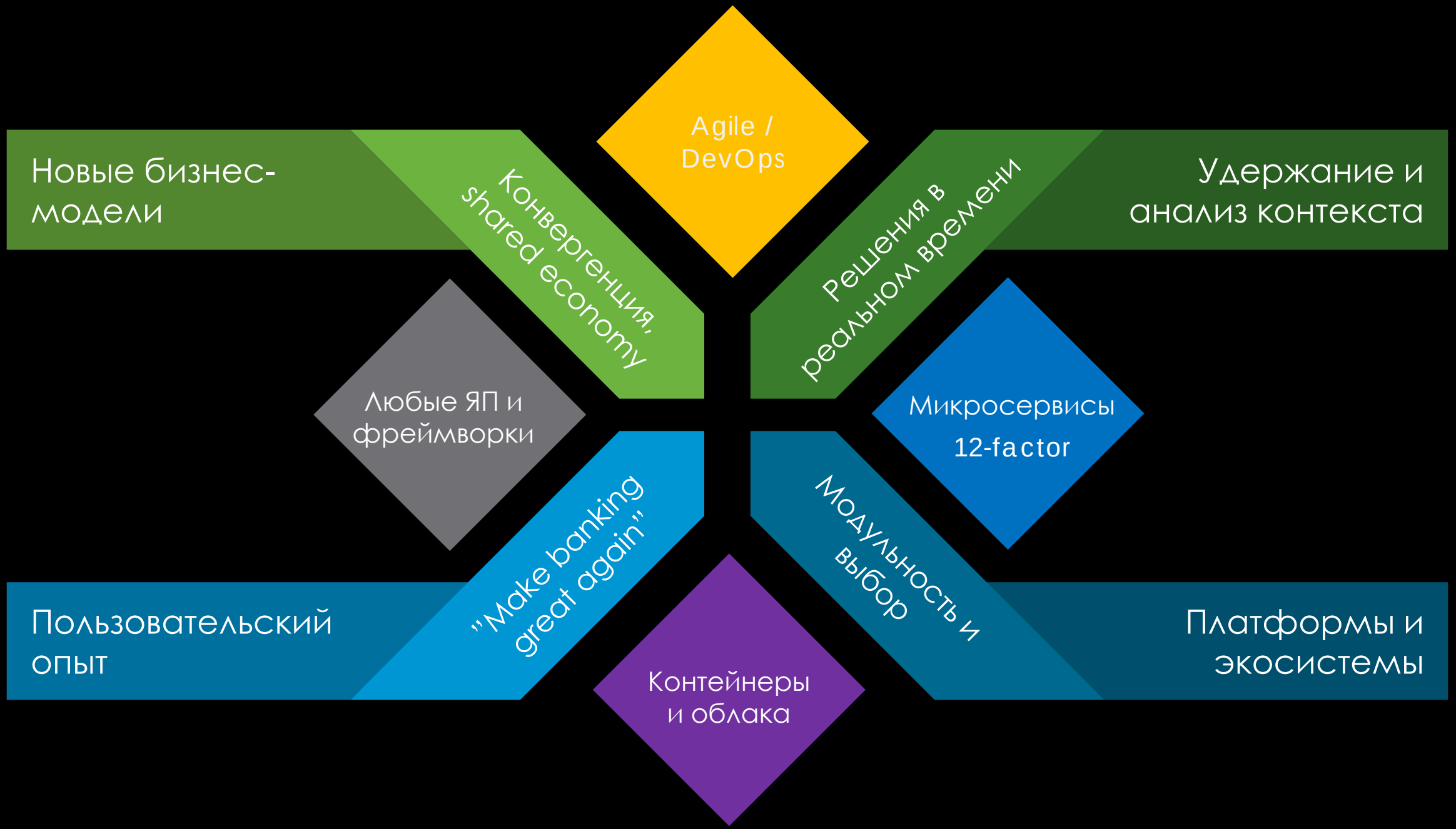
Артем Гениев

13 февраля 2018

vmware®

О сколько нам открытий чудных

Готовят просвещенья дух…


Agile / DevOps
Новые бизнес-модели
Конвергенция, shared economy
Решения в реальном времени
Удержание и анализ контекста
Любые ЯП и фреймворки
Микросервисы 12-factor
"Make banking great again"
Модульность и выбор
Пользовательский опыт
Контейнеры и облака
Платформы и экосистемы

О КАКОЙ ДИНАМИКЕ ИЗМЕНЕНИЙ МЫ ГОВОРИМ?

Wealthfront

Управление инвестициями, инвестиционный консалтинг

$ 97M

AUM 2013

$ 7B

AUM 2017

30

Релизов / день

30 000

Релизов / 3 года

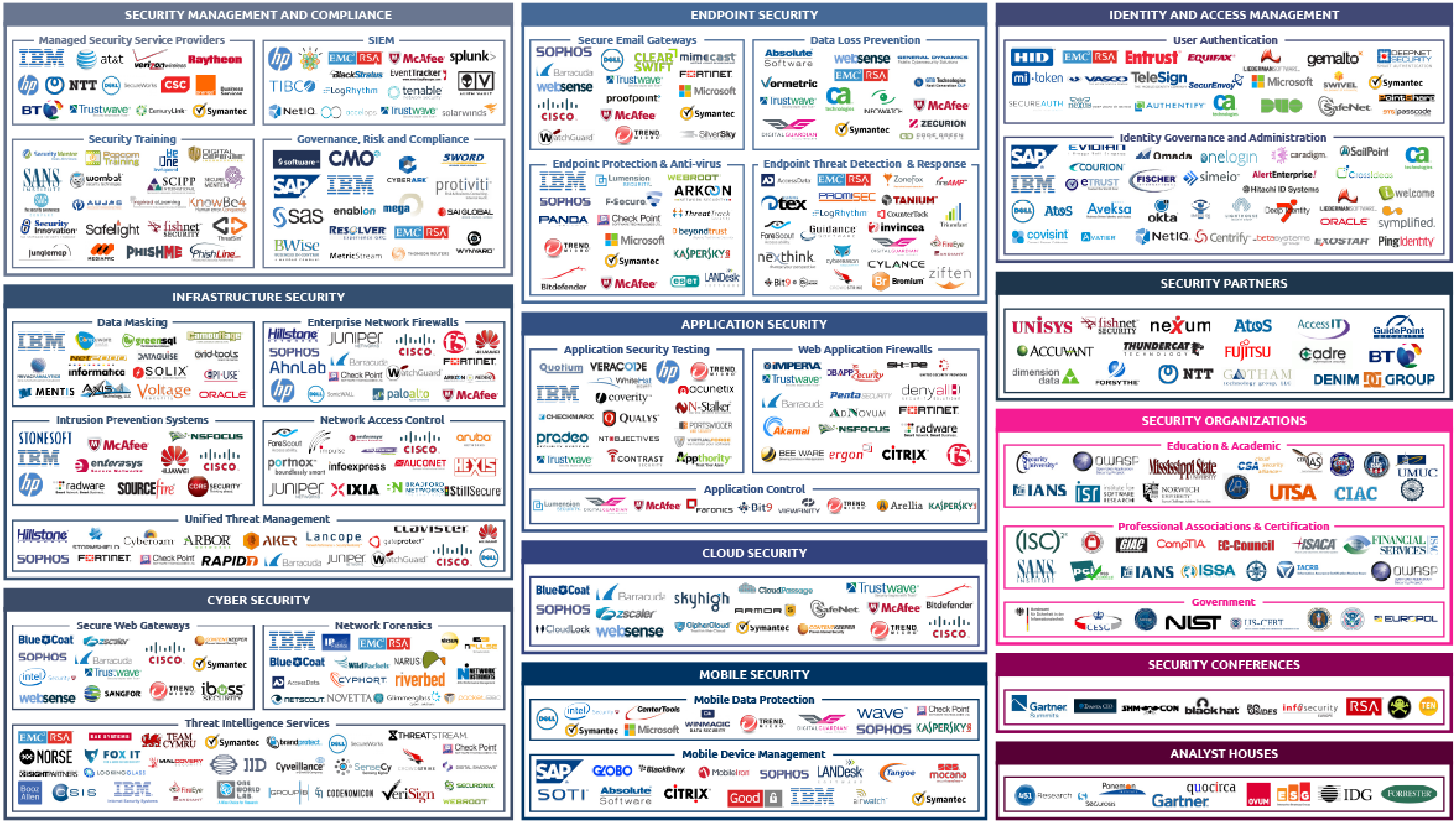
КОНТРОЛЬ

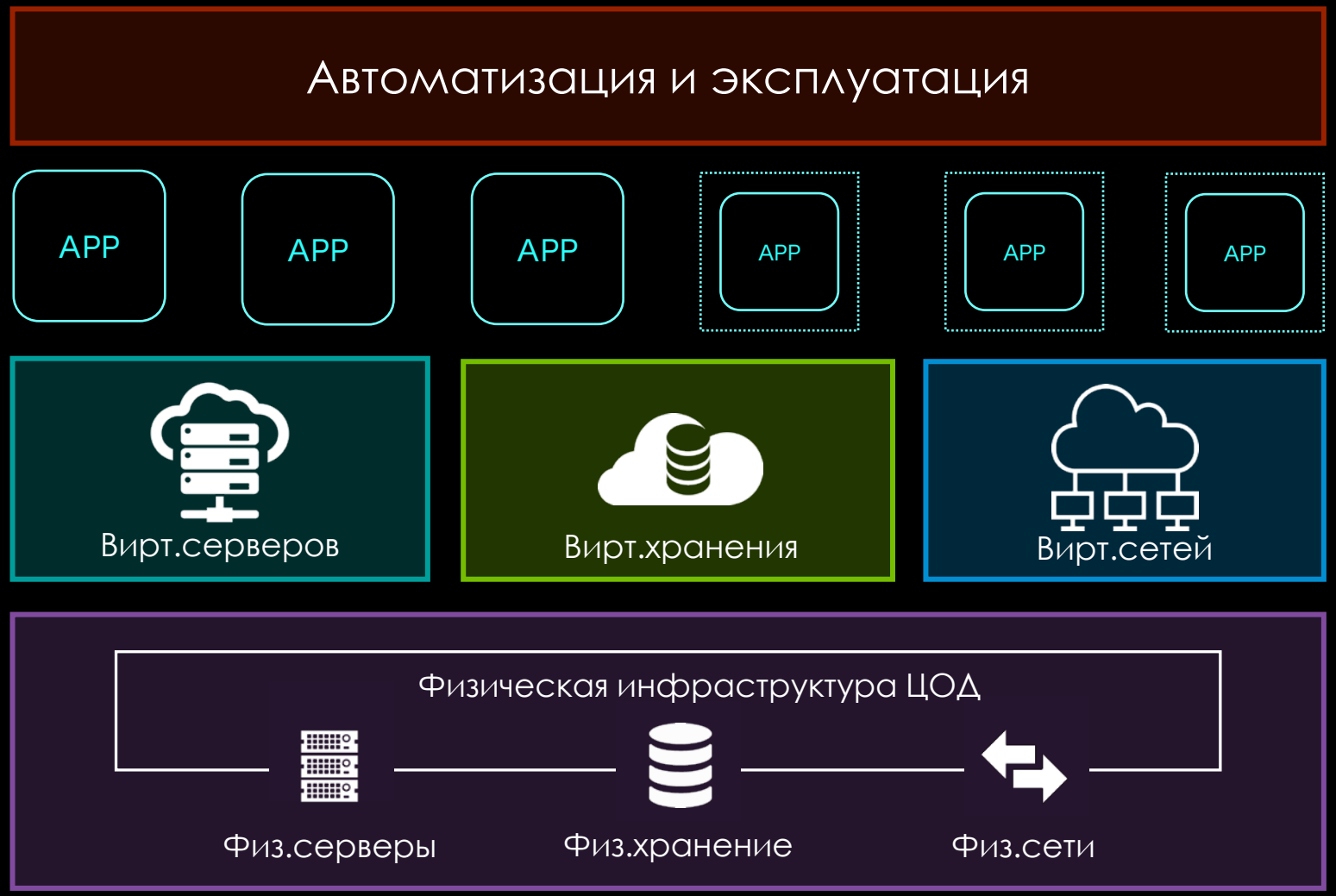
ИЛИ

СВОБОДА?

Какой велосипед изобрели на сей раз?

Принцип наименьших привилегий


SECURITY MANAGEMENT AND COMPLIANCE
Managed Security Service Providers
SIEM
Security Training
Governance, Risk and Compliance
INFRASTRUCTURE SECURITY
Data Masking
Enterprise Network Firewalls
Intrusion Prevention Systems
Network Access Control
Unified Threat Management
CYBER SECURITY
Secure Web Gateways
Network Forensics
Threat Intelligence Services
ENDPOINT SECURITY
Secure Email Gateways
Data Loss Prevention
Endpoint Protection & Anti-virus
Endpoint Threat Detection & Response
APPLICATION SECURITY
Application Security Testing
Web Application Firewalls
Application Control
CLOUD SECURITY
MOBILE SECURITY
Mobile Data Protection
Mobile Device Management
IDENTITY AND ACCESS MANAGEMENT
User Authentication
Identity Governance and Administration
SECURITY PARTNERS
SECURITY ORGANIZATIONS
Education & Academic
Professional Associations & Certification
Government
SECURITY CONFERENCES
ANALYST HOUSES



Программно-определяемый Центр Обработки Данных (SDDC)

Модели угроз

Векторы атаки

Объекты защиты

Уязвимости

Полномочия

ЧТО ТАКОЕ ВИРТУАЛИЗАЦИЯ

ДЛЯ СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ?

ФЗ-152

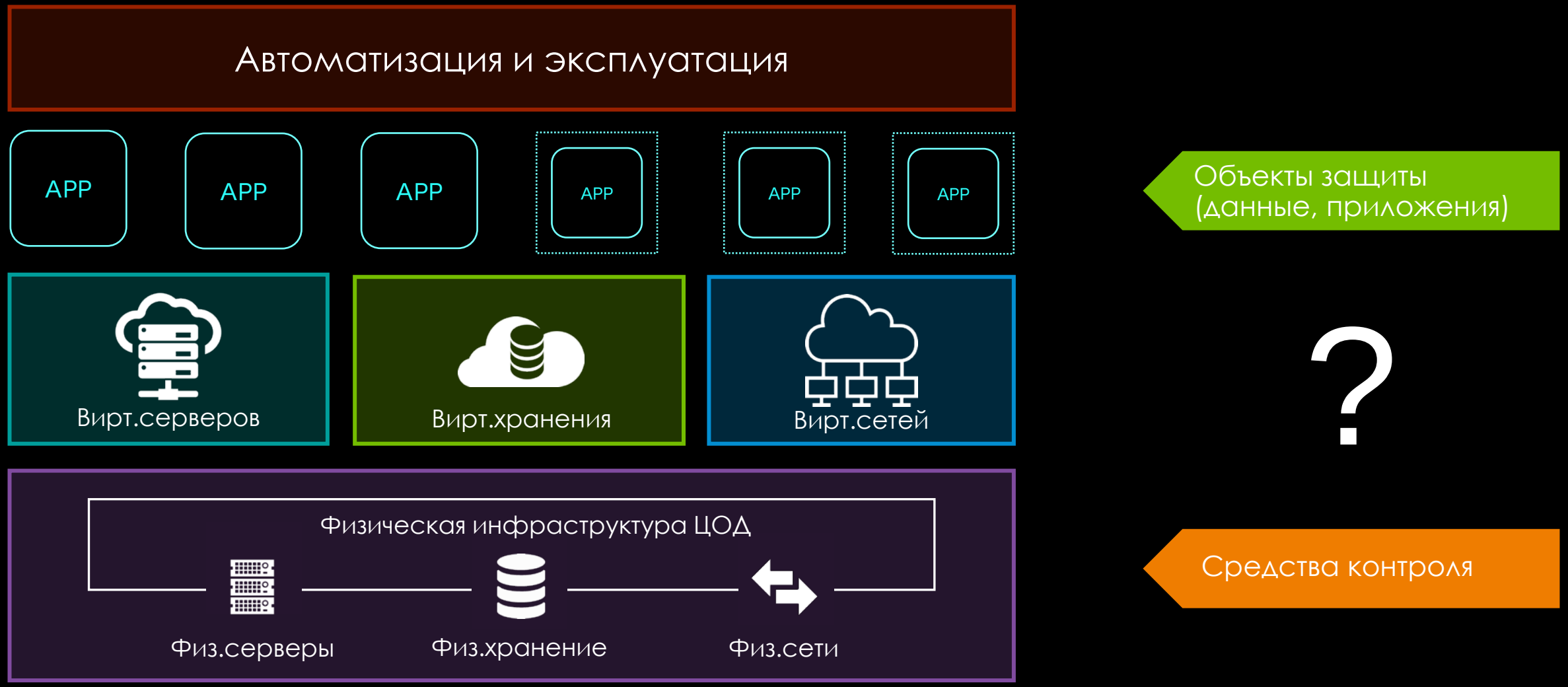
Стратегия защиты

Управление учетными данными

PCI-DSS

DRP/BCP


GOLDILOCKS ZONE


Автоматизация и эксплуатация
APP
APP
APP
APP
APP
APP
Вирт.серверов
Вирт.хранения
Вирт.сетей
Физическая инфраструктура ЦОД
Физ.серверы
Физ.хранение
Физ.сети
Объекты защиты (данные, приложения)
?
Средства контроля

Вирт.серверов

Вирт.хранения

Вирт.сетей

Наименьшие привилегии для SD - инфраструктуры

ПРИНЦИП НАИМЕНЬШИХ ПРИВИЛЕГИЙ ДЛЯ СЕТЕЙ

ZERO TRUST SECURITY

Доступ должен быть безопасным

БЕЗОПАСНЫЙ ДОСТУП КО ВСЕМ РЕСУРСАМ ВНЕ ЗАВИСИМОСТИ ОТ РАСПОЛОЖЕНИЯ

Стратегия минимальных полномочий

И ЖЕСТКИЙ КОНТРОЛЬ ДОСТУПА

Анализировать и журналировать

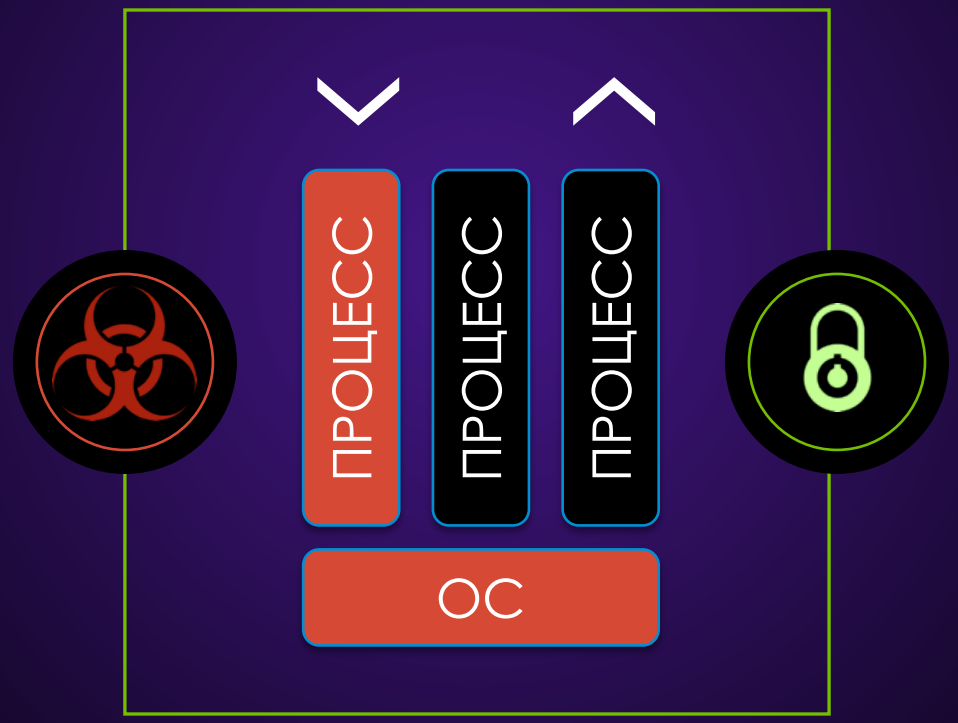
ВЕСЬ СЕТЕВОЙ ТРАФИК

ПРИНЦИП НАИМЕНЬШИХ ПРИВИЛЕГИЙ ДЛЯ ВЫЧИСЛЕНИЙ

ИЩЕМ «ПЛОХОЕ»

ПРИНЦИП НАИМЕНЬШИХ ПРИВИЛЕГИЙ ДЛЯ ВЫЧИСЛЕНИЙ

ИЩЕМ «ПЛОХОЕ»



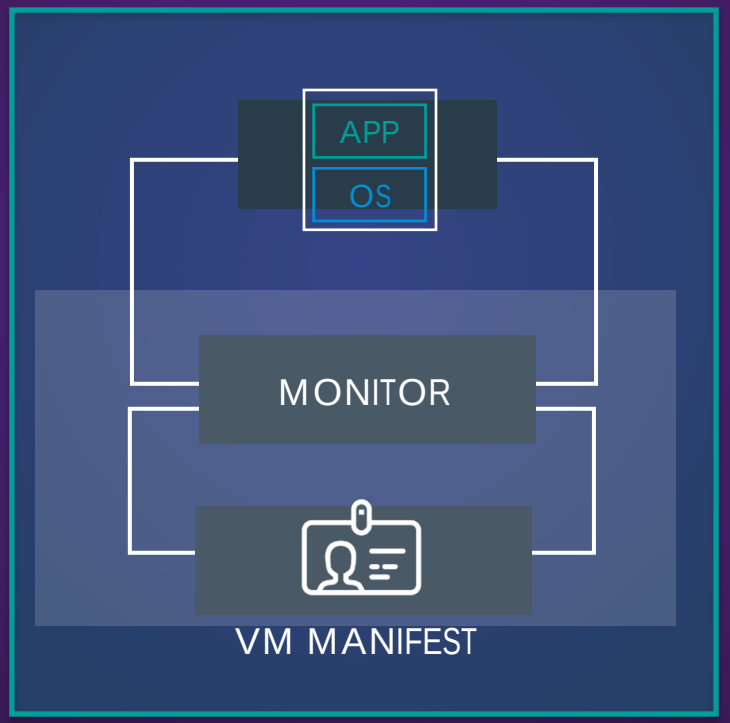
ГАРАНТИРУЕМ «ХОРОШЕЕ»


Перевернуть модель безопасности
Ищем «плохое»
Гарантируем «хорошее»
Благодаря принципу наименьших привилегий

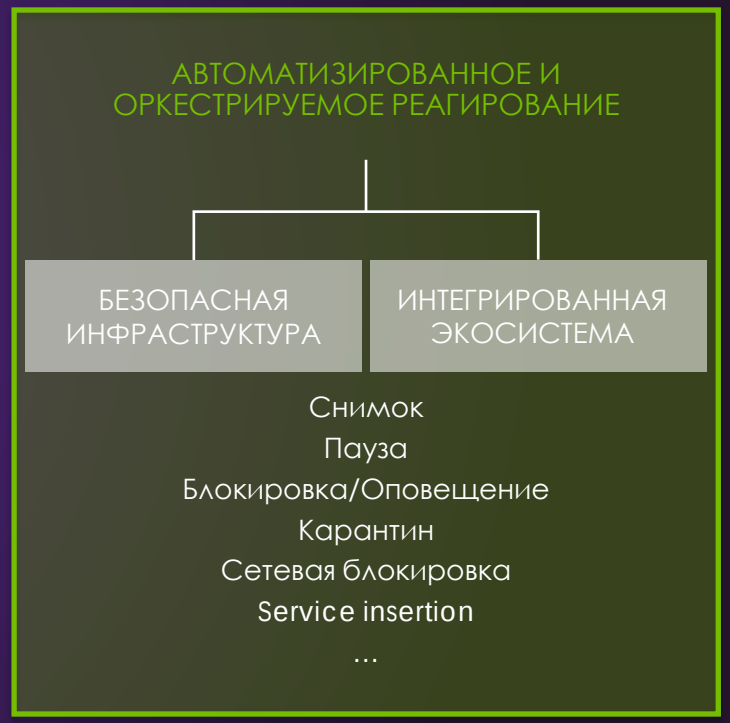
ИИ + SDDC = ИБ²

ГАРАНТИРОВАНИЕ НОРМАЛЬНОГО СОСТОЯНИЯ ПУТЕМ АНАЛИЗА КОНТЕКСТА

ЭТАЛОН



ОБНАРУЖЕНИЕ



РЕАГИРОВАНИЕ



Кибер-гигиена

IPS, IDS, FW, WAF…

SIEM, SOC

Безопасность конечных устройств

Интегрированная экосистема


Вирт.серверов


Вирт.хранения


Вирт.сетей

Наименьшие привилегии для SD - инфраструктуры

DevOps + ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

С ПРОГРАММНО-ОПРЕДЕЛЯЕМЫМ ЦОД

PenTest:

- 3 недели работы
- 300 страниц отчета

WAF:

- ”Continuous configuration”

Анализ кода

- Настройка
- Запуск
- Анализ

Классика

ИЛИ

Контроль за слабо меняющимися компонентами:

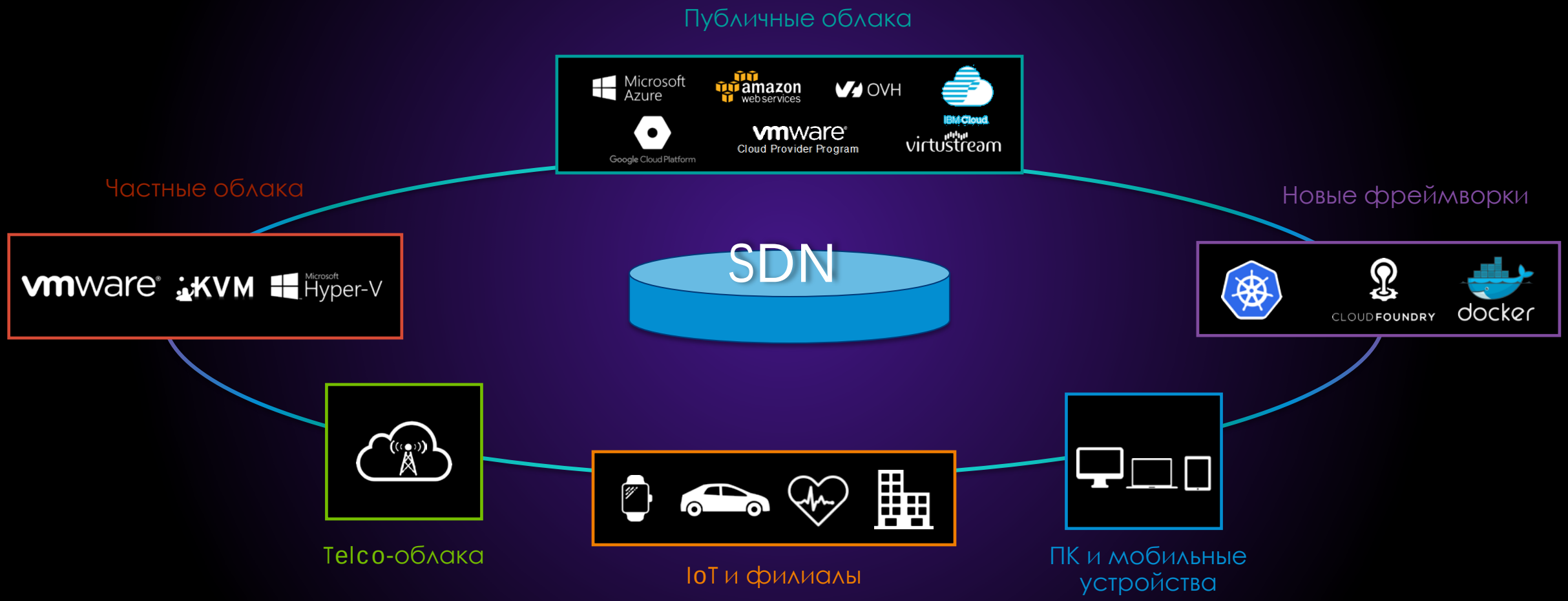
- Шаблоны / блюпринты, образы ОС и контейнеров

Там же применяются политики безопасности.

Плюс немного «классики» ;)

“Shift Left”

ОТ ДАТАЦЕНТРОВ…
К ЦЕНТРАМ ДАННЫХ



Спасибо за внимание

ageniev@vmware.com

vmware®