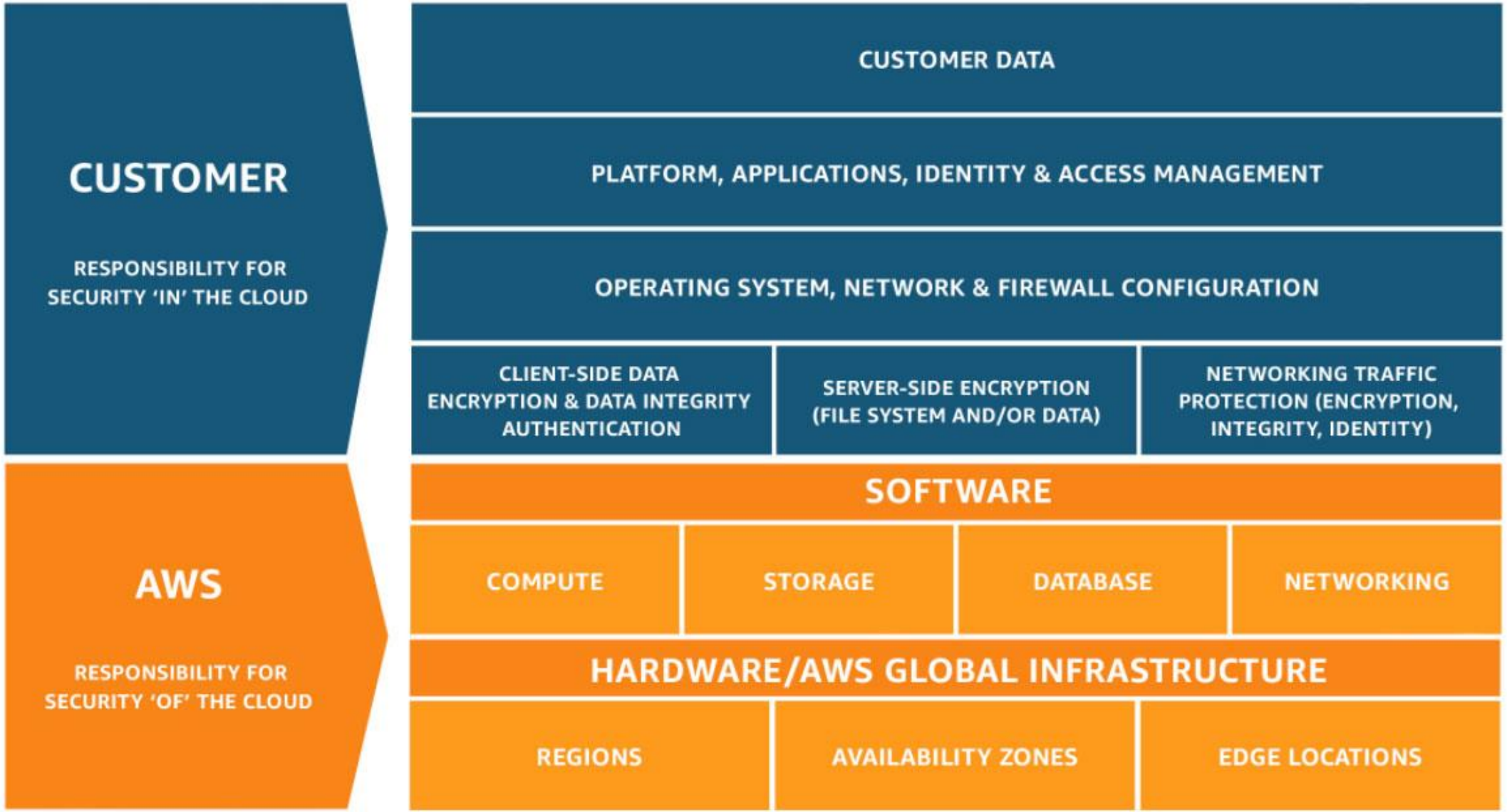
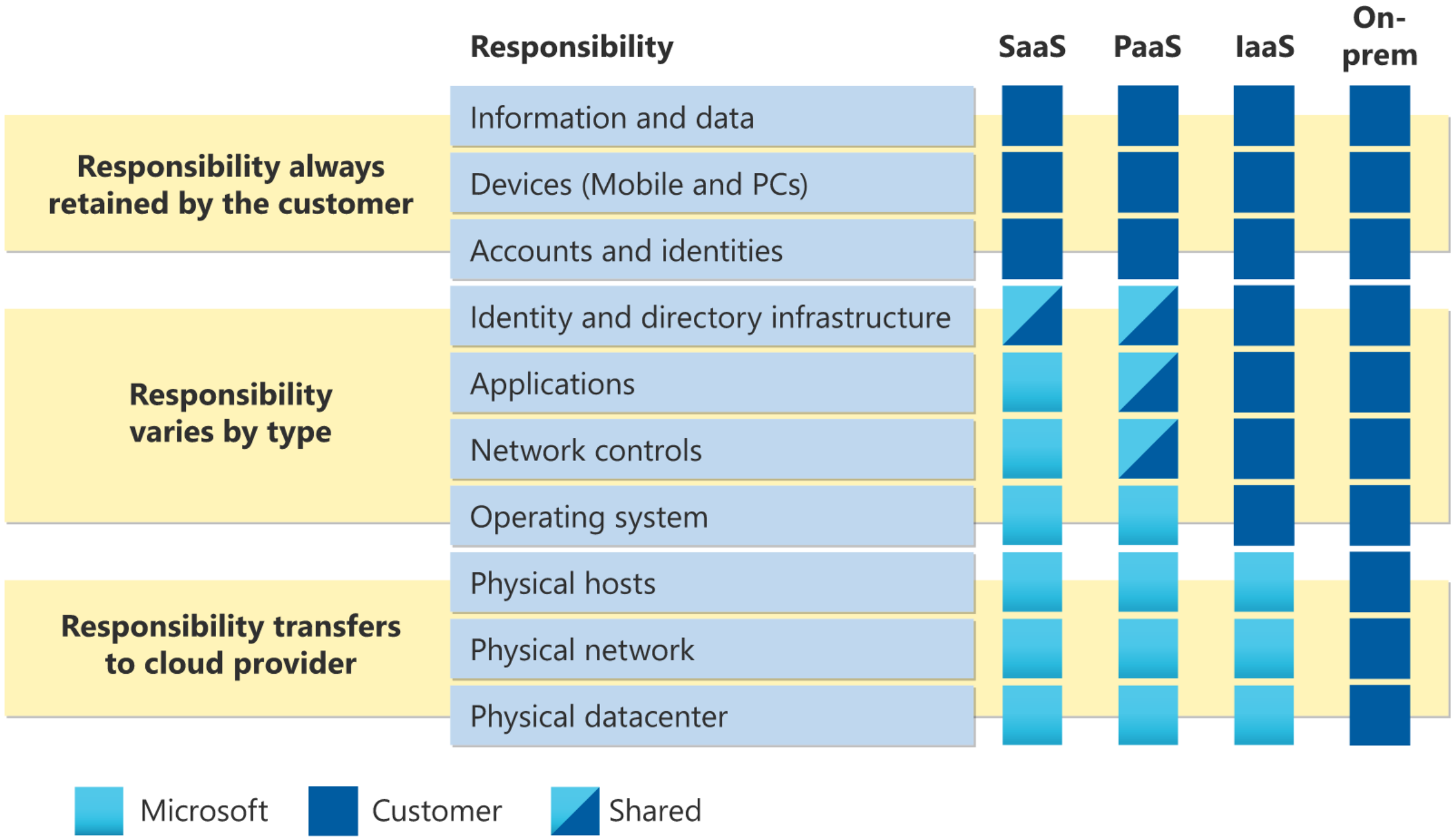
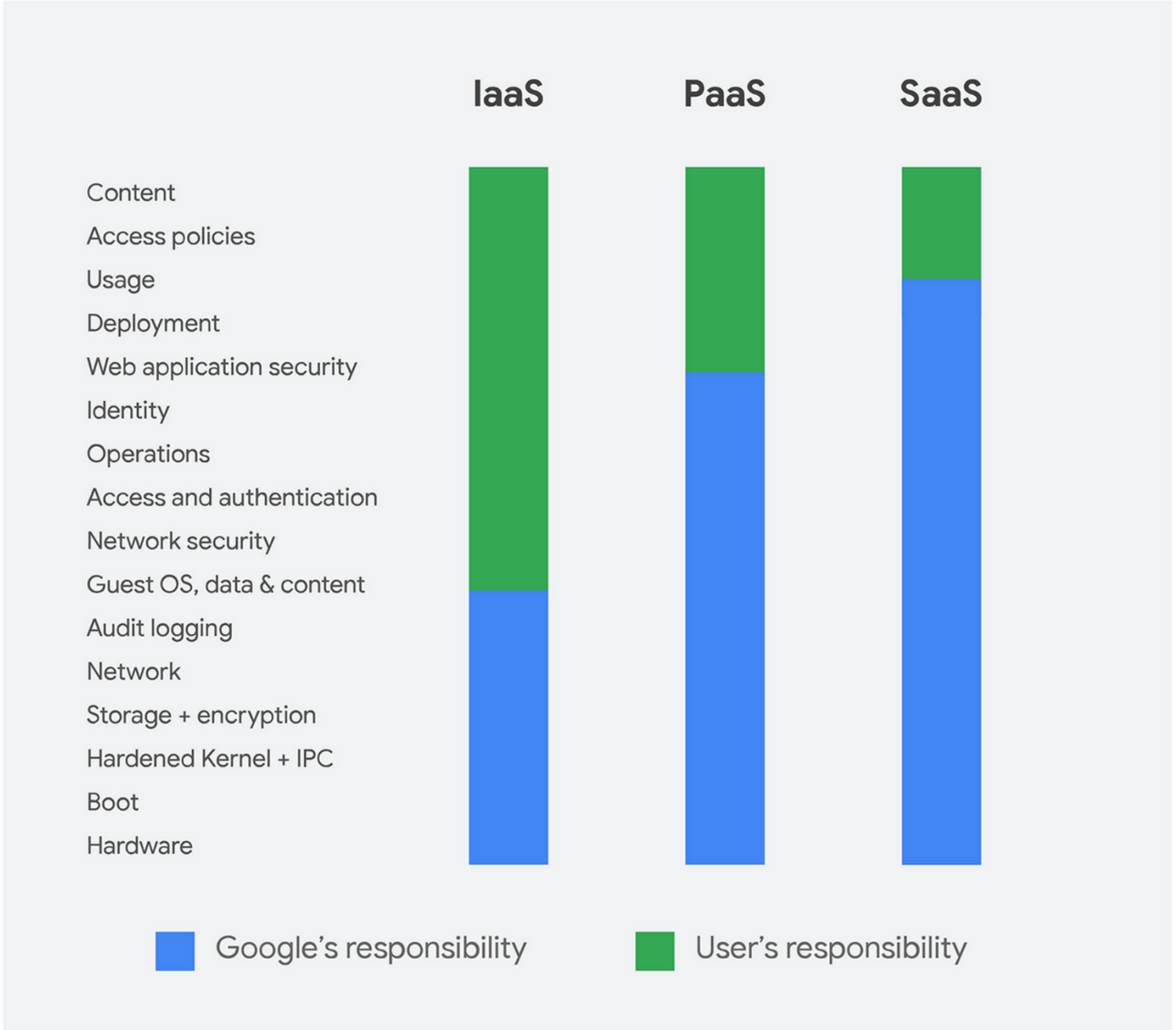
Shared Responsibility Model

РАЗДЕЛЕНИЕ ОТВЕТСТВЕННОСТИ ЗА ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ







- Клиент
- Yandex.Cloud

	Собственная инфраструктура	IaaS	PaaS
Управление доступом к данным	○	○	○
Безопасность ОС и приложений	○	○	●
Сетевая безопасность (Overlay)	○	○	●
Резервное копирование	○	○	●
Шифрование	○	○	●
Логи аудита	○	●	●
Безопасность хранилища данных и оборудования	○	●	●
Сетевая безопасность (Underlay)	○	●	●
Физическая безопасность и катастрофоустойчивость (DR)	○	●	●

Разделение ответственности в облаках

Клиент
отвечает за безопасность **«внутри»** облака

Облачная платформа
отвечает за безопасность **«самого»** облака

Данные клиента

Пользователи, роли, разрешения

Приложения

Платформа

Операционная система, шифрование, сетевой трафик

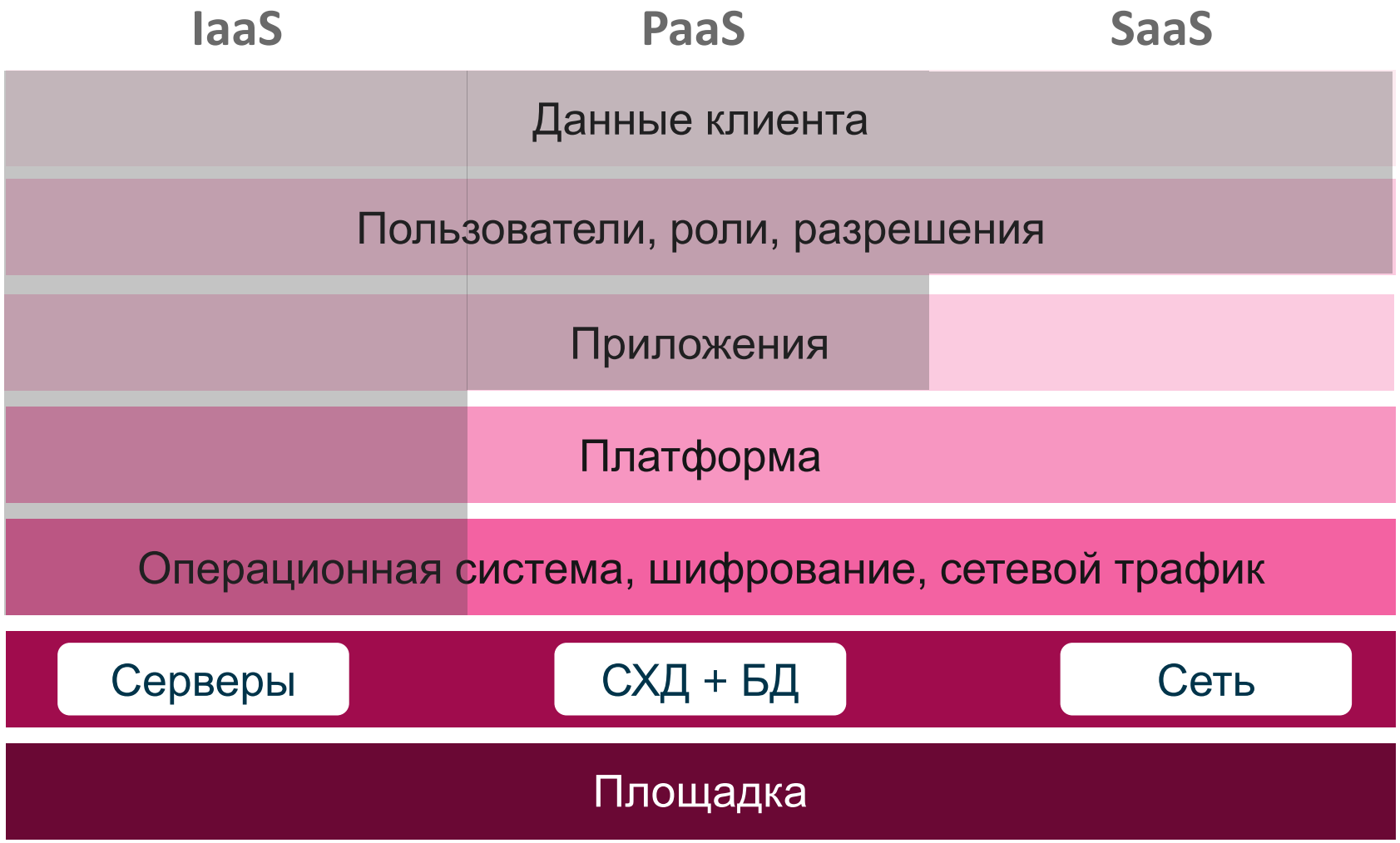
Серверы | СХД + БД | Сеть

Площадка

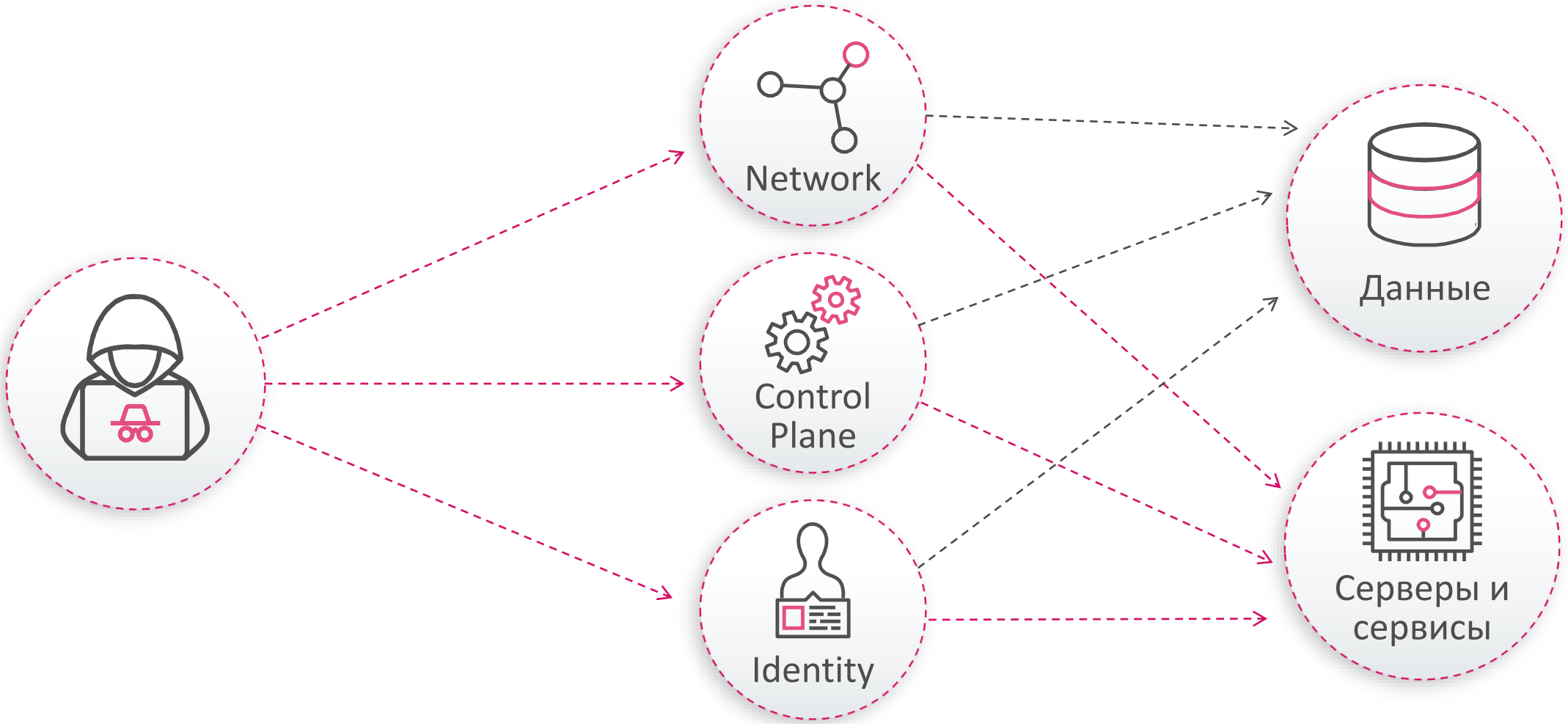
Разделение ответственности в облаках

Клиент
отвечает за безопасность **«внутри»** облака

Облачная платформа
отвечает за безопасность **«самого»** облака



Векторы атак на облако



За что отвечает провайдер облака

- Физическая безопасность
- Катастрофоустойчивость
- Шифрование данных
- Соответствие стандартам – compliance
  - ФЗ-152, GDPR, PCI DSS и др.

Какие инструменты безопасности обычно предоставляет провайдер

- Identity and Access Management (IAM)
- Журналы и аудит действий
- Key Management Services (KMS)
- Изоляция сети клиента
- AntiDDoS
- Security Groups, NACL
- Интеграция с партнерскими сервисами

Favorites

Add favorites by clicking on the star next to the service name.

Recently visited

Console Home

All services

Compute
EC2
Lightsail
Lambda
Batch
Elastic Beanstalk
Serverless Application Repository
AWS Outposts
EC2 Image Builder
AWS App Runner

Containers
Elastic Container Registry
Elastic Container Service
Elastic Kubernetes Service
Red Hat OpenShift Service on AWS

Storage
S3
EFS
FSx
S3 Glacier
Storage Gateway
AWS Backup

Database
RDS
DynamoDB
ElastiCache
Neptune
Amazon QLDB
Amazon DocumentDB
Amazon Keyspaces
Amazon Timestream
Amazon MemoryDB for Redis

Migration & Transfer

Customer Enablement
AWS IQ
Support
Managed Services
Activate for Startups

Robotics
AWS RoboMaker

Blockchain
Amazon Managed Blockchain

Satellite
Ground Station

Quantum Technologies
Amazon Braket

Management & Governance
AWS Organizations
CloudWatch
AWS Auto Scaling
CloudFormation
CloudTrail
Config
OpsWorks
Service Catalog
Systems Manager
AWS AppConfig
Trusted Advisor
Control Tower
AWS License Manager
AWS Well-Architected Tool
Personal Health Dashboard
AWS Chatbot
Launch Wizard
AWS Compute Optimizer

Machine Learning
Amazon SageMaker
Amazon Augmented AI
Amazon CodeGuru
Amazon DevOps Guru
Amazon Comprehend
Amazon Forecast
Amazon Fraud Detector
Amazon Kendra
Amazon Lex
Amazon Personalize
Amazon Polly
Amazon Rekognition
Amazon Textract
Amazon Transcribe
Amazon Translate
AWS DeepComposer
AWS DeepLens
AWS DeepRacer
AWS Panorama
Amazon Monitron
Amazon HealthLake
Amazon Lookout for Vision
Amazon Lookout for Equipment
Amazon Lookout for Metrics

Analytics
Athena
Amazon Redshift
EMR
CloudSearch
Amazon OpenSearch Service (successor to Amazon Elasticsearch Service)
Kinesis
QuickSight
Data Pipeline
AWS Data Exchange

AWS Cost Management
AWS Cost Explorer
AWS Budgets
AWS Marketplace Subscriptions
AWS Application Cost Profiler

Front-end Web & Mobile
AWS Amplify
AWS AppSync
Device Farm
Amazon Location Service

AR & VR
Amazon Sumerian

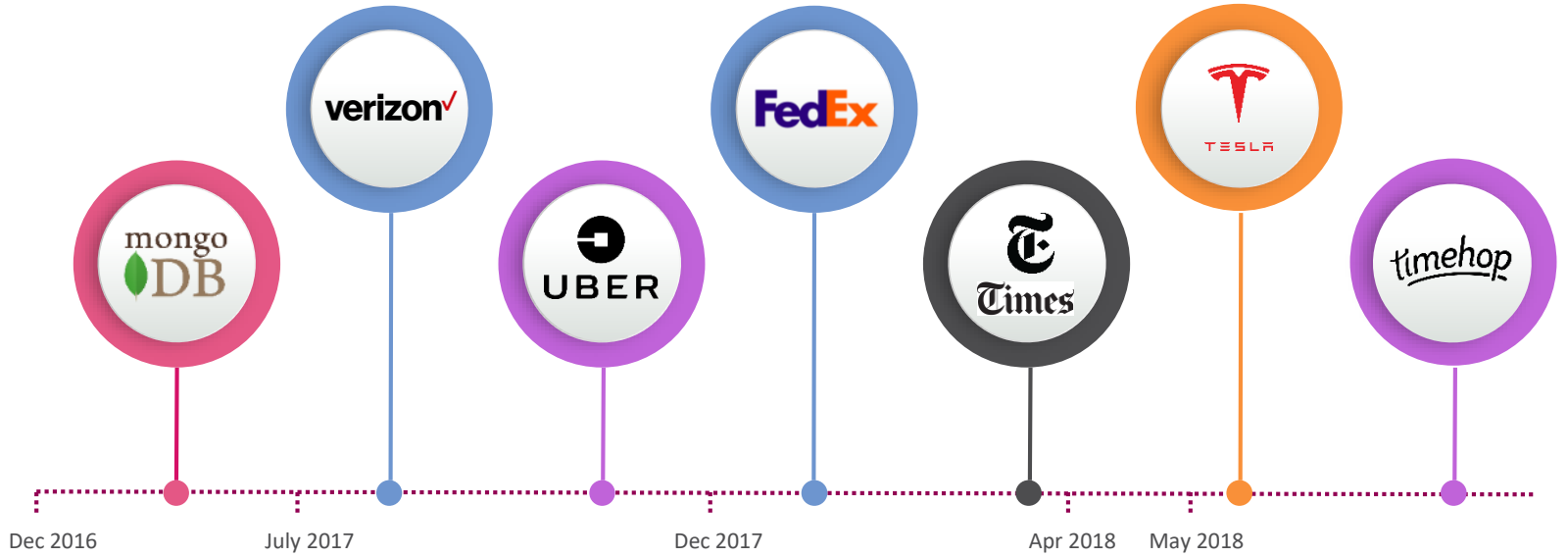
Application Integration
Step Functions
Amazon AppFlow
Amazon EventBridge
Amazon MQ
Simple Notification Service
Simple Queue Service
SWF
Managed Apache Airflow

Business Applications
Amazon Connect
Amazon Pinpoint
Amazon Honeycode
Amazon Chime
Amazon Simple Email Service
Amazon WorkDocs
Amazon WorkMail
Alexa for Business

End User Computing
WorkSpaces

Ошибки и злонамеренные изменения в конфигурации облаков обходятся дорого

- Данные клиента
- **Уровень управления**
- Облачные сервисы провайдера



- Уязвимости
- Криптомайнеры
- Украденные учетки
- Ошибки конфигурации

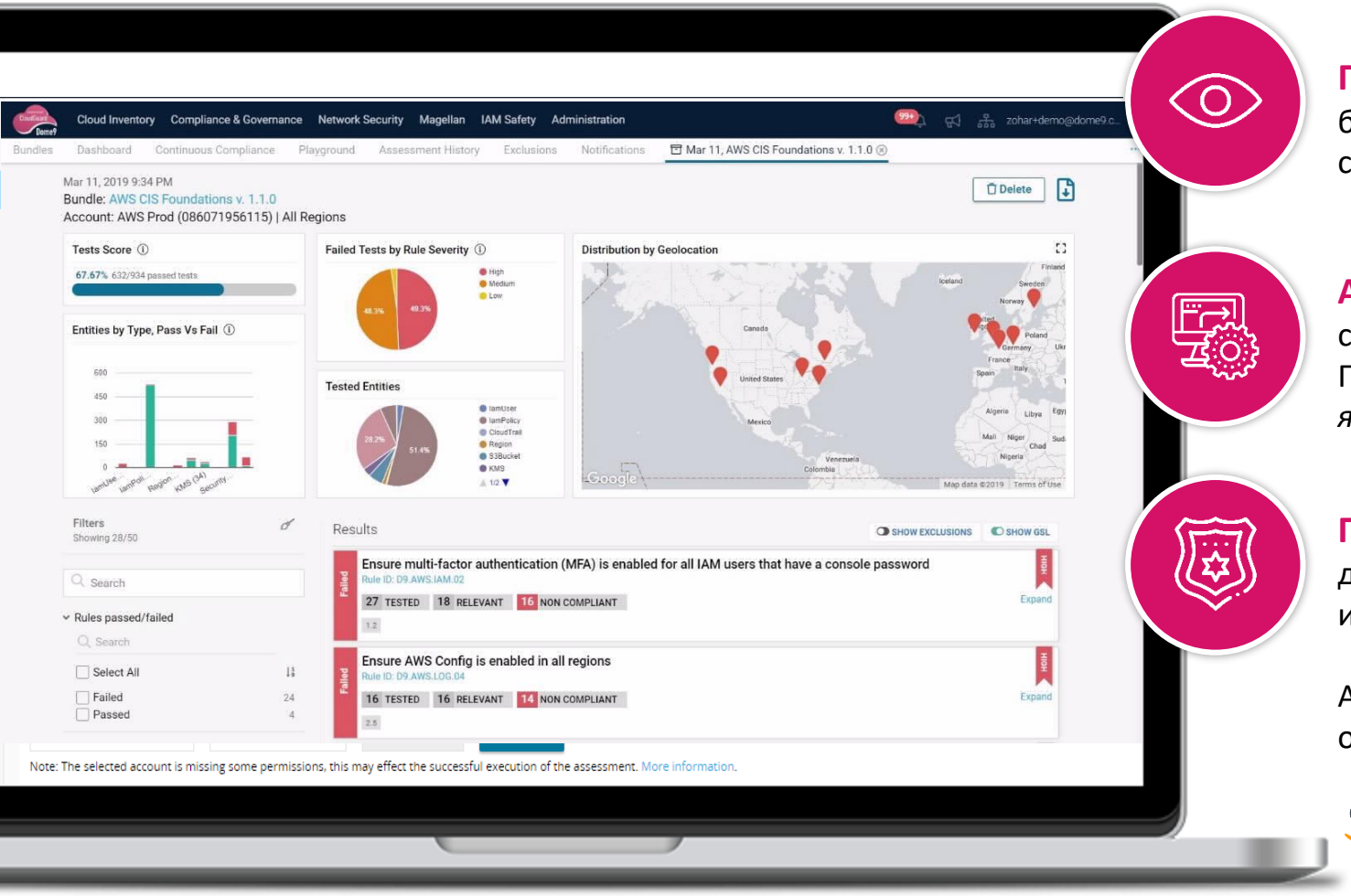
FORTUNE

THE LEDGER • TESLA

Tesla Hackers Hijacked Amazon Cloud Account to Mine Cryptocurrency

Контроль настроек в облаке

Оценка безопасности, уровней доступа и политик для публичных облаков и контейнеров



Полный контроль над всеми серверами, функциями, бакетами, политиками безопасности, IAM, виртуальными сетями и аккаунтами в публичных облаках и K8S.

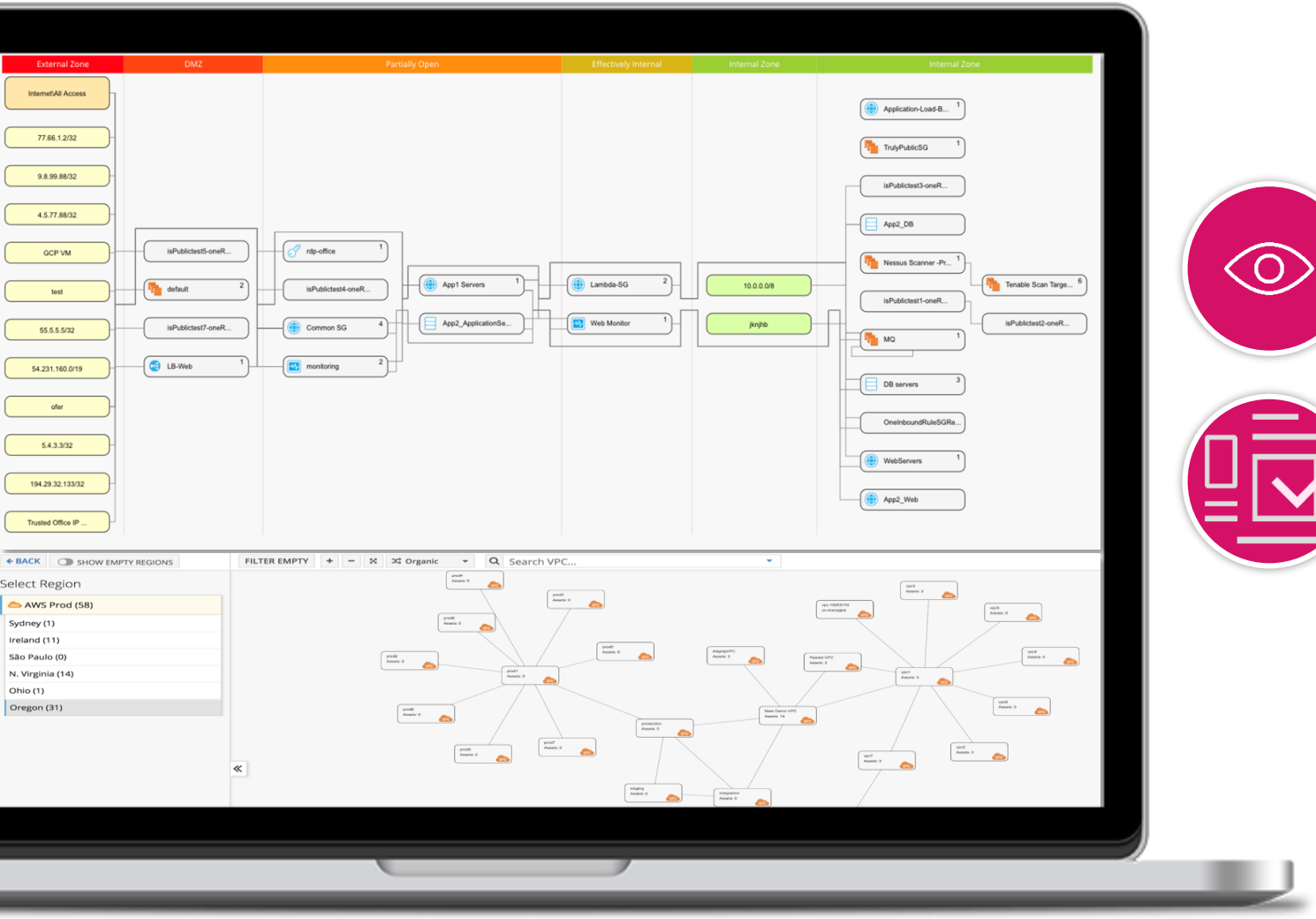
Автоматические отчеты на соответствие отраслевых стандартов защиты и лучших практик в ИБ.
Простая и понятная настройка правил на «*человеческом языке*»

Предотвращение *кражи* учетных *записей*, неавторизованного доступа к облакам, некорректных или злонамеренных изменений настроек безопасности.

Автоматическое исправление и коррекция политик и настроек облачных ресурсов

aws Google Cloud Azure

Визуализация сети облака

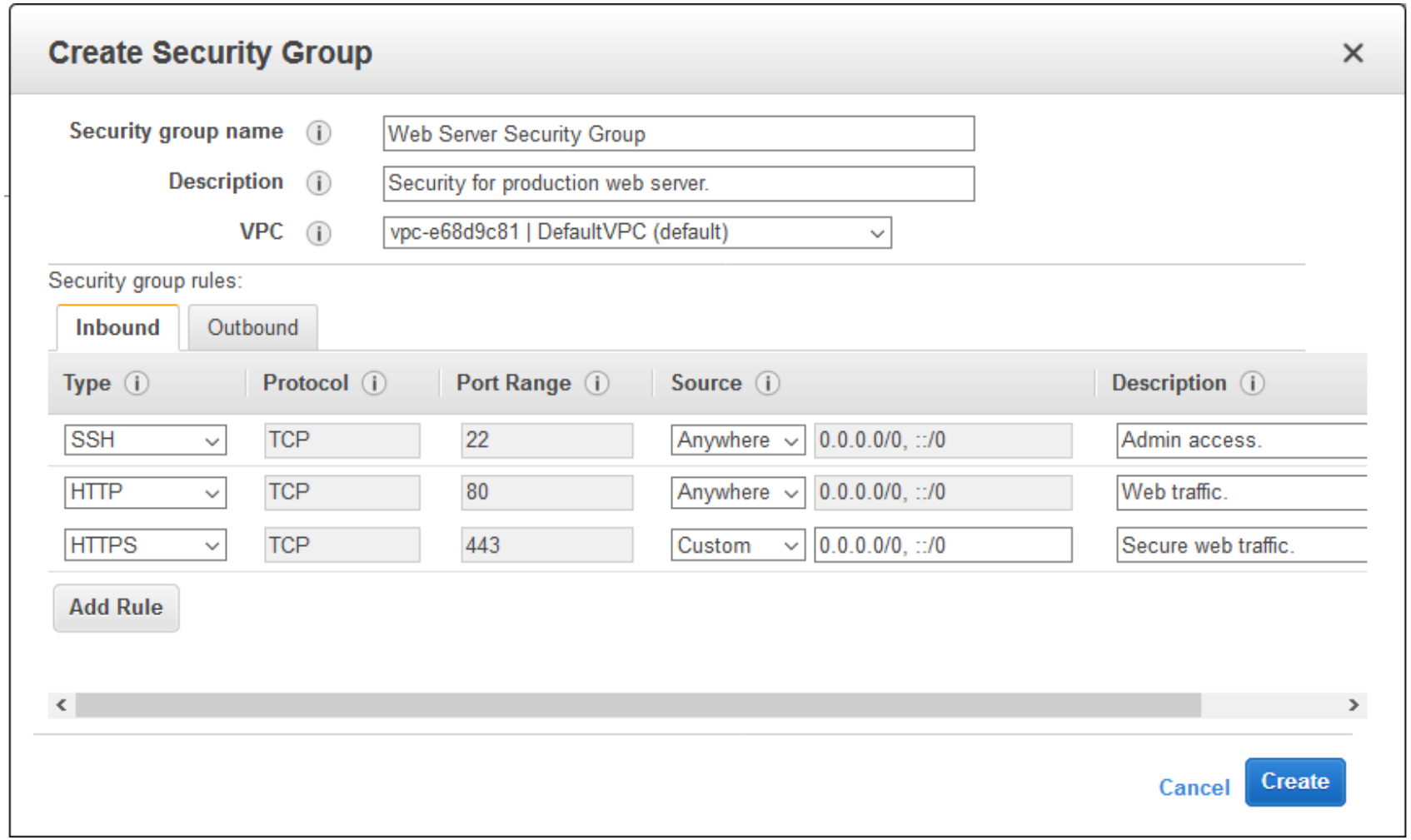


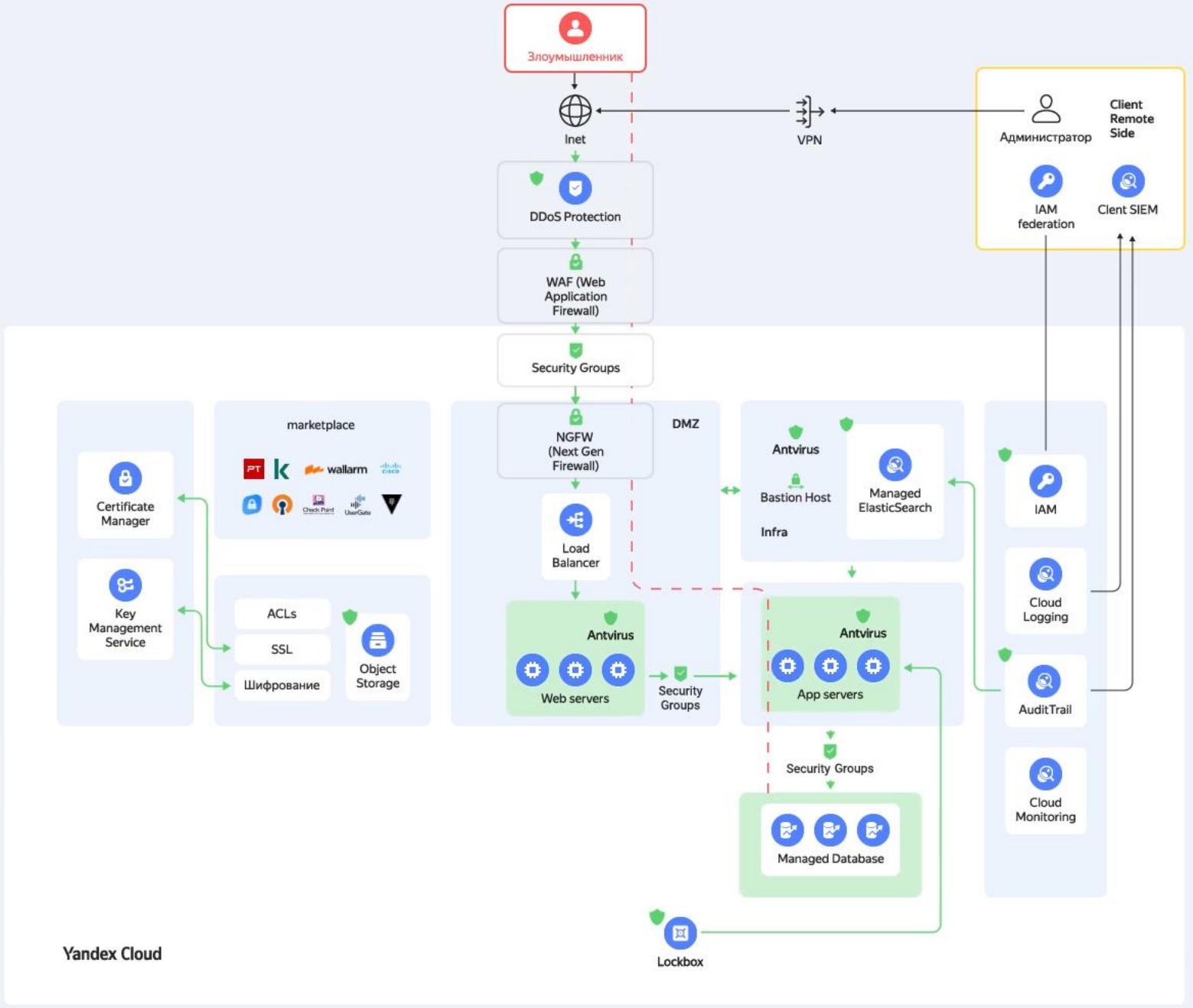
Визуализация всей сети вашего облака, включая виртуальный машины, фукнции, регионы.

Быстрая оценка уязвимых и открытых для интернета ресурсов

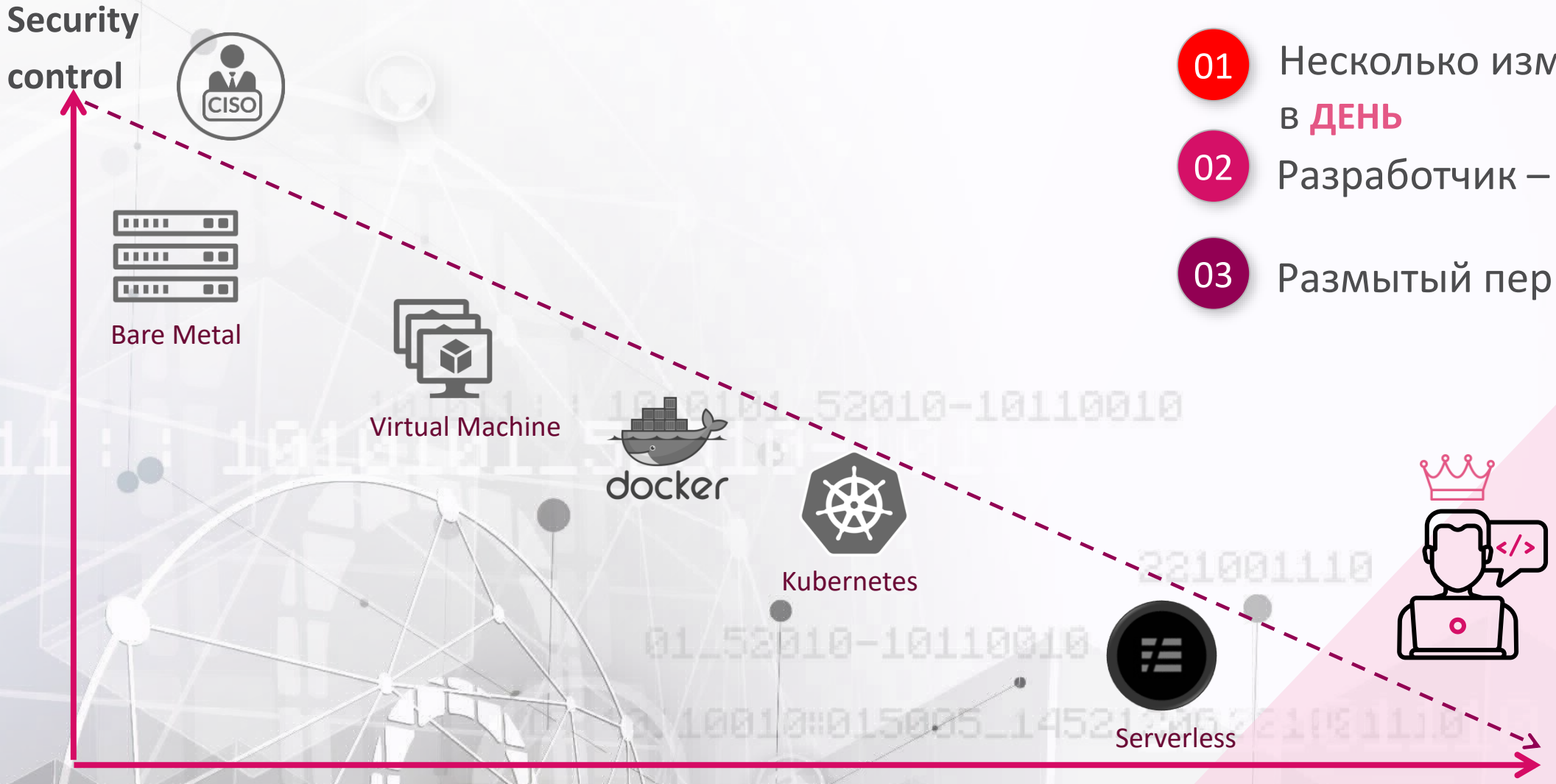
Анализ пиринга регионов

Встроенный инструмент - Security Group




Злоумышленник
Inet
VPN
Администратор
Client Remote Side
IAM federation
Client SIEM
DDoS Protection
WAF (Web Application Firewall)
Security Groups
NGFW (Next Gen Firewall)
DMZ
Load Balancer
marketplace
Certificate Manager
Key Management Service
ACLs
SSL
Шифрование
Object Storage
Antvirus
Web servers
Security Groups
Antvirus
Bastion Host
Infra
Managed ElasticSearch
Antvirus
App servers
Security Groups
Managed Database
IAM
Cloud Logging
AuditTrail
Cloud Monitoring
Lockbox
Yandex Cloud

Технологии развиваются, а безопасность?



01 Несколько изменений в **ДЕНЬ**

02 Разработчик – царь горы

03 Размытый периметр

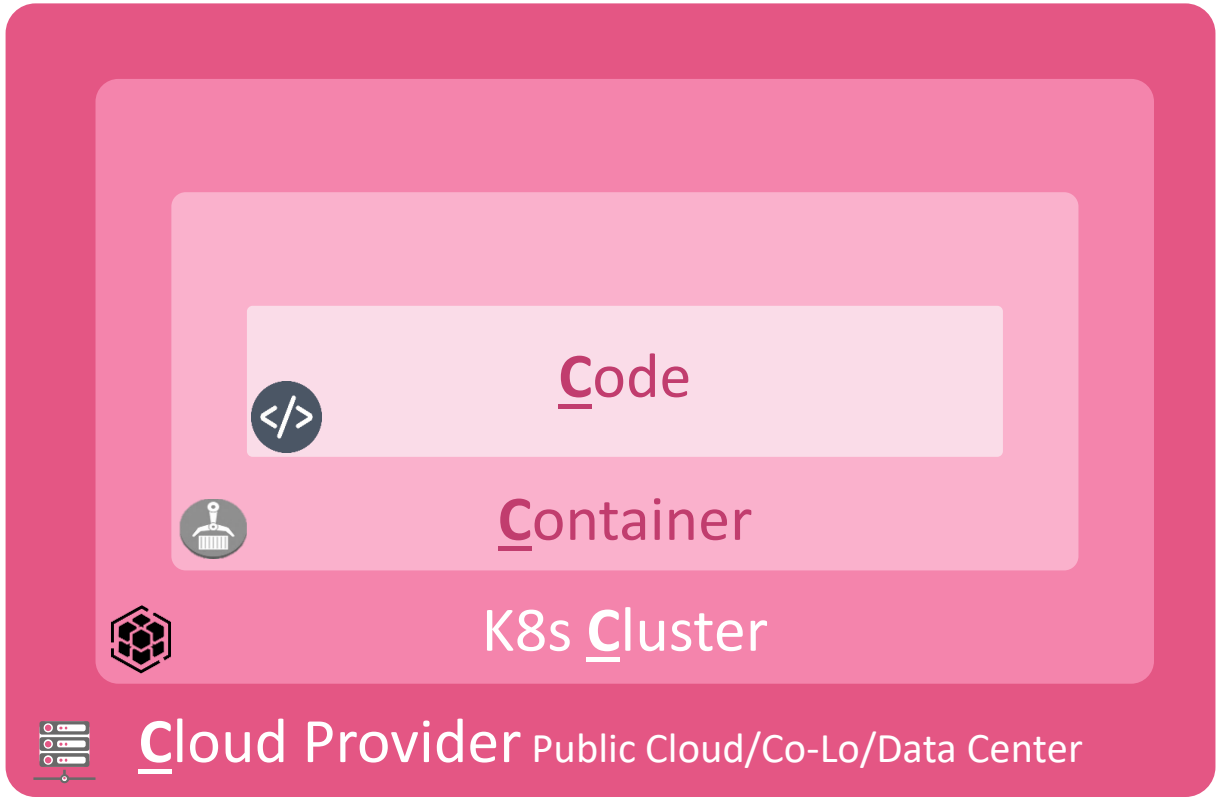
Модель «The 4C's of Cloud Native security»: Концепция защиты облаков

Модель защиты «4C»

Эшелонированный подход:

- Защищаем облачный периметр
- Сами ресурсы внутри облака
- Контейнеры/приложения
- Сам код этих приложений

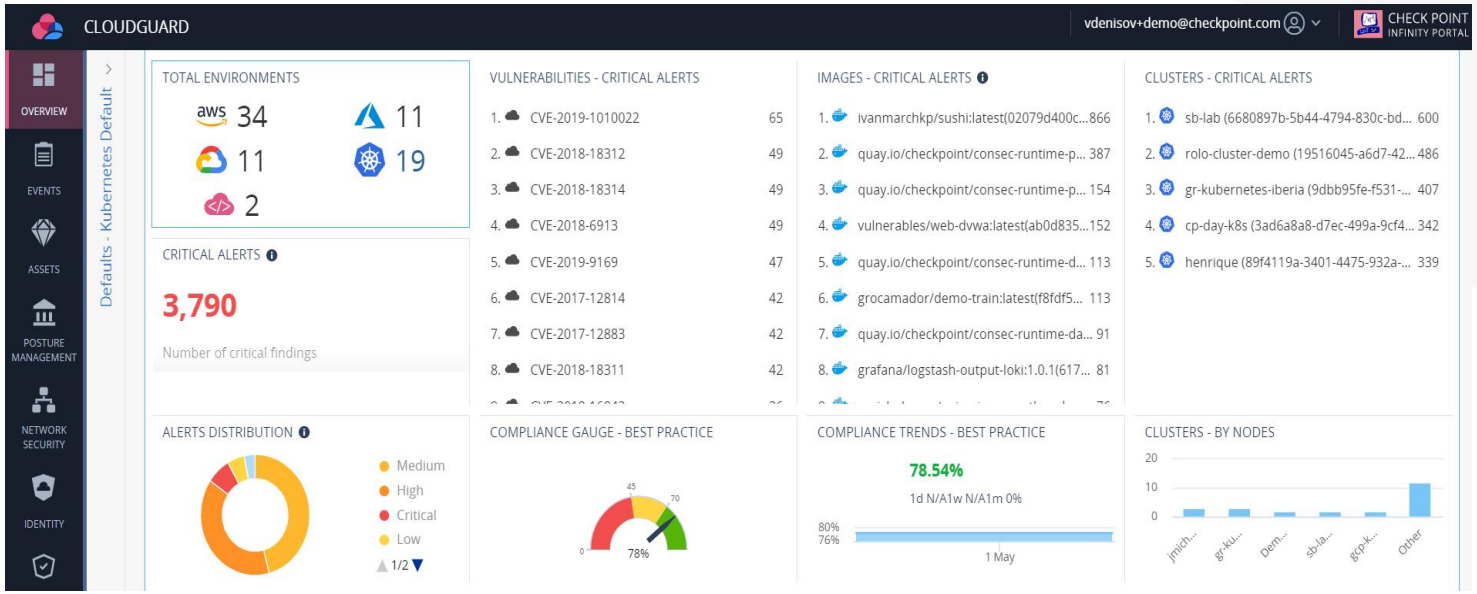
Дизайн защиты: Данный подход позволяет обеспечить безопасность на всех этапах жизни современных сервисов



https://kubernetes.io/docs/concepts/security/overview/

Workload protection

- Анализ уязвимостей и исходного кода внутри контейнеров
- Поиск аномалий в поведении запущенных контейнеров
- Защита API k8s от неавторизованных изменений (Admission controller)

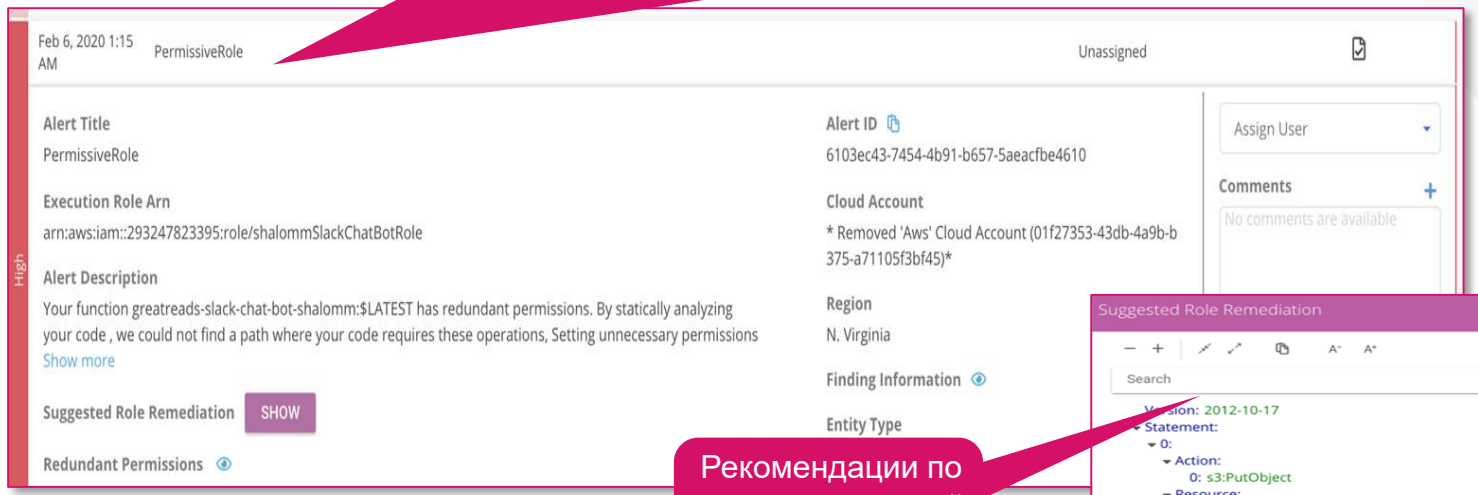


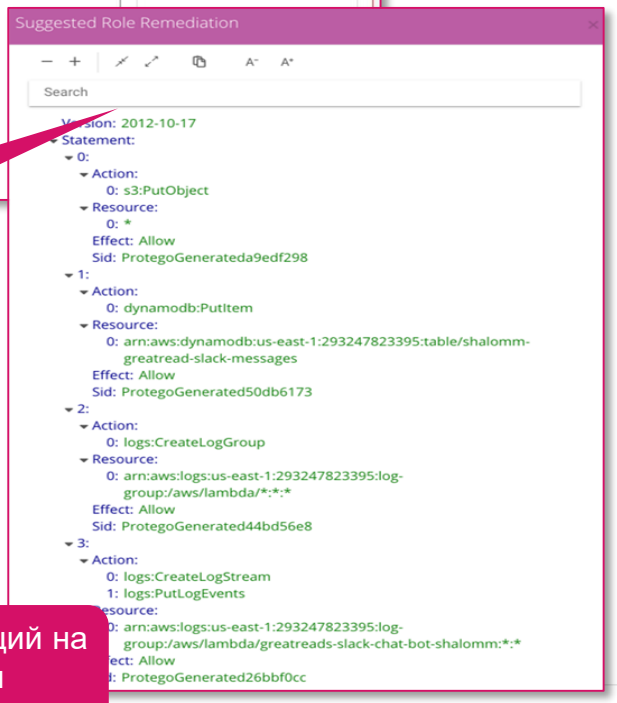
Защита облачных функций

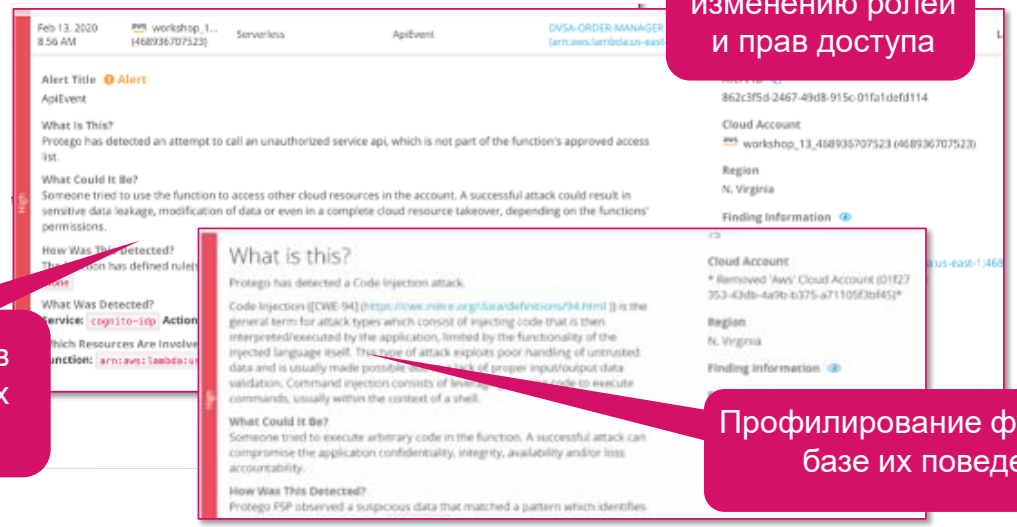
Автоматическая защита Runtime

- ✓ Постоянное сканирование на поиск уязвимостей и прав доступа
- ✓ Визуализация взаимодействия с другими сервисами AWS
- ✓ Профилирование и whitelisting

Анализ уязвимостей в коде и слишком широких прав доступа





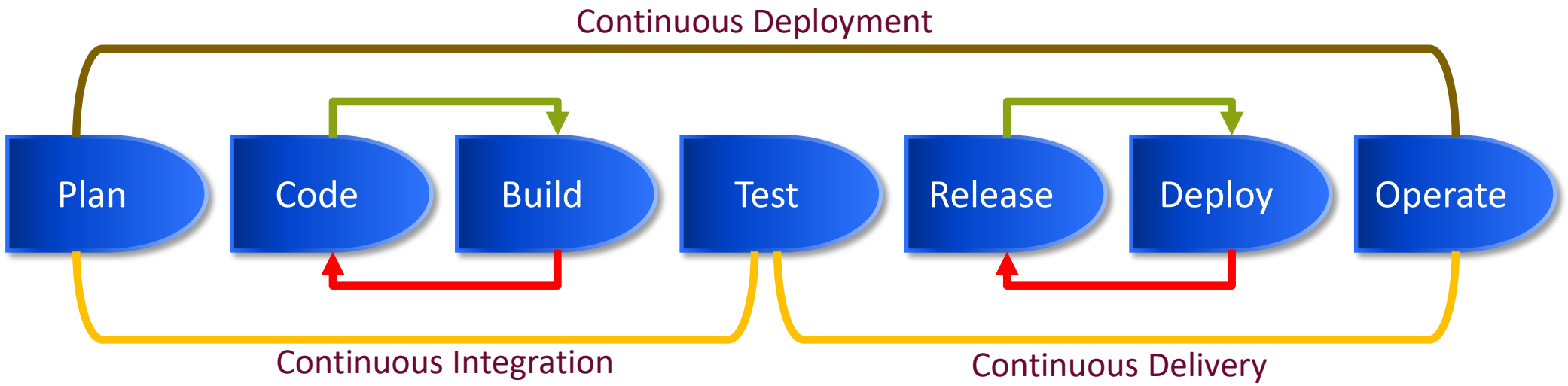


Рекомендации по изменению ролей и прав доступа

Анализ вызовов API и сторонних ресурсов

Профилирование функций на базе их поведения

Continuous Integration / Continuous Deployment



Актуальные вопросы

- Кто чем управляет?
- Кто за чем наблюдает?
- Кто отвечает за резервное копирование?
- Кто отвечает за отказоустойчивость?
- Кто что делает в случае инцидента?