Возможен ли безопасный доступ к сервисам?

$whoami

Алексей Федулаев

- В ИБ с 2011 года
- Head of Cloud Native Security
- Спикер крупнейших российских конференций, ведущий подкастов SafeCode Live
- Автор канала Ever Secure @ever_secure
- Делаю мир безопаснее =)

$whoami

Георг Гаал

- 10+ лет в IT
- из них не менее 7 - в крупных enterprise / fintech
- Покусан безопасниками, становлюсь как они
- Спикер крупнейших международных конференций и образовательных проектов
- Стараюсь дружить dev, ops и sec

О чем сегодня поговорим?

- о типичных ошибках и как делать не надо
- что делать и кто виноват?
- о наших надеждах на светлое будущее

Что такое безопасный доступ к сервисам?

это такой доступ, который

- мы можем в любой момент времени отозвать
- мы знаем кто, где и почему (и что делал)
- масштабируется
- есть breaking glass (если все сломалось - можем зайти)

тут должна быть пикча с аварийным выходом и молотком

Hotfix

Чем плох ssh?

- используется не по назначению - и для административных задач, и просто для пользователей, а еще для автоматизаций

Чем плох ssh?

- используется не по назначению - и для административных задач, и просто для пользователей, а еще для автоматизаций
- следовательно, нужны разные роли для “пользователей”

Чем плох ssh?

- используется не по назначению - и для административных задач, и просто для пользователей, а еще для автоматизаций
- следовательно, нужны разные роли для “пользователей”
- но на уровне Linux их нет! Модель доступов линукс - тривиальна (группа? пользователь? selinux?). Если есть доступ к серверу - взлом easy (== локальный терминал)

Чем плох ssh?

- используется не по назначению - и для административных задач, и просто для пользователей, а еще для автоматизаций
- следовательно, нужны разные роли для “пользователей”
- но на уровне Linux их нет! Модель доступов линукс - тривиальна (группа? пользователь? selinux?). Если есть доступ к серверу - взлом easy (== локальный терминал)
- по классике - вход по паролям (не устойчиво к брутфорсу)

Чем плох ssh?

- используется не по назначению - и для административных задач, и просто для пользователей, а еще для автоматизаций
- следовательно, нужны разные роли для “пользователей”
- но на уровне Linux их нет! Модель доступов линукс - тривиальна (группа? пользователь? selinux?). Если есть доступ к серверу - взлом easy (== локальный терминал)
- по классике - вход по паролям (не устойчиво к брутфорсу)
- давайте сделаем fail2ban

Чем плох ssh?

- используется не по назначению - и для административных задач, и просто для пользователей, а еще для автоматизаций
- следовательно, нужны разные роли для “пользователей”
- но на уровне Linux их нет! Модель доступов линукс - тривиальна (группа? пользователь? selinux?). Если есть доступ к серверу - взлом easy (== локальный терминал)
- по классике - вход по паролям (не устойчиво к брутфорсу)
- давайте сделаем fail2ban
- кто поумнее - ключи (по сути тот же пароль, только длинный, как менеджить и отзывать)

Чем плох ssh?

- используется не по назначению - и для административных задач, и просто для пользователей, а еще для автоматизаций
- следовательно, нужны разные роли для “пользователей”
- но на уровне Linux их нет! Модель доступов линукс - тривиальна (группа? пользователь? selinux?). Если есть доступ к серверу - взлом easy (== локальный терминал)
- по классике - вход по паролям (не устойчиво к брутфорсу)
- давайте сделаем fail2ban
- кто поумнее - ключи (по сути тот же пароль, только длинный, как менеджить и отзывать)
- сертификаты? сложно!

ЛУЧШИЙ ПАРОЛЬ - КОТОРОГО НЕТ!!!

Current state:

1. Создали сервак

Current state:

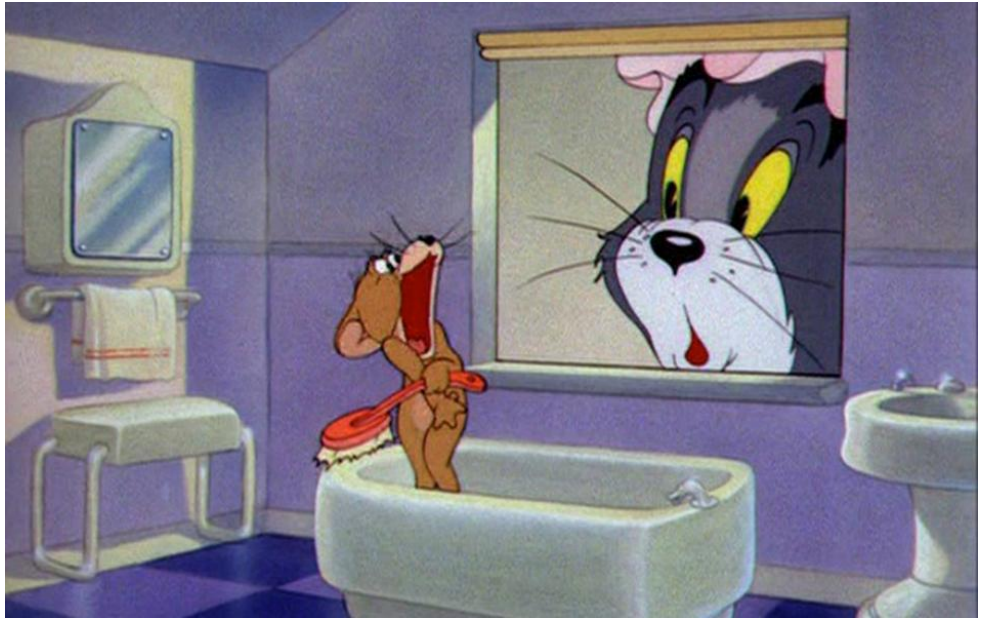
1. Создали сервак
2. Достаточный чтобы запустить linux =)

Current state:

1. Создали сервак
2. Делаем ssh

Current state:

1. Создали сервак
2. Делаем ssh
3. Выставляем в интернет



Current state:

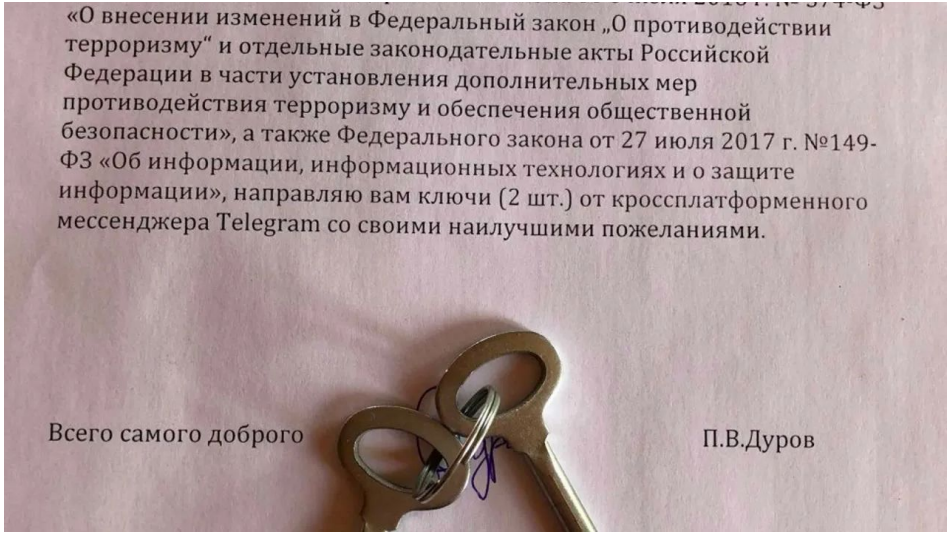
1. Создали сервак
2. Делаем ssh
3. Выставляем в интернет
4. Базово под паролем

Current state:

1. Создали сервак
2. Делаем ssh
3. Выставляем в интернет
4. Базово под паролем
5. Если повезет - root недоступен

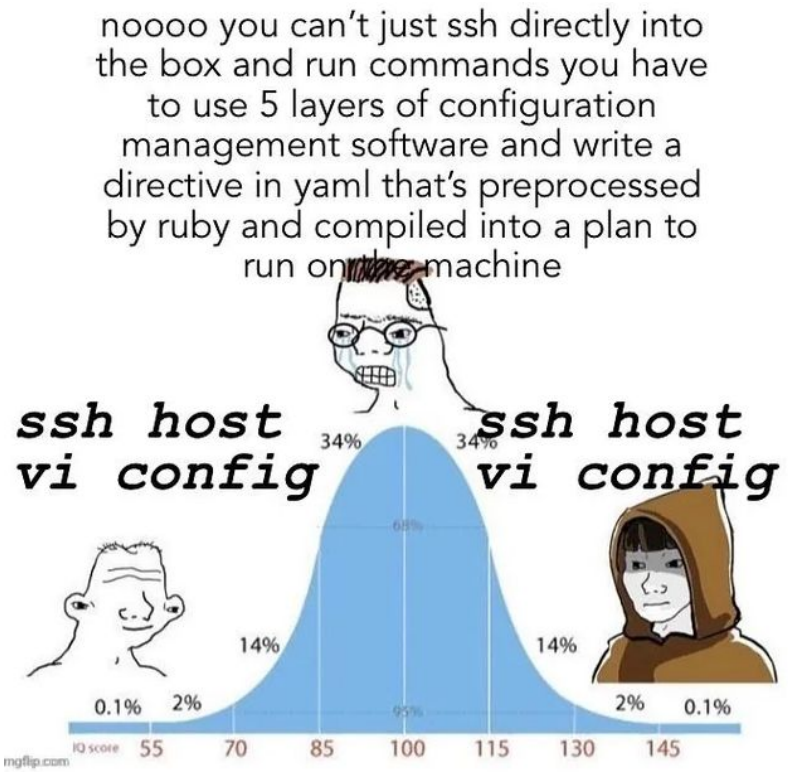
Current state:

1. Создали сервак
2. Делаем ssh
3. Выставляем в интернет
4. Базово под паролем
5. Если повезет - root недоступен
6. Вход по ключам?



Current state:

1. Создали сервак
2. Делаем ssh
3. Выставляем в интернет
4. Базово под паролем
5. Если повезет - root недоступен
6. Вход по ключам?
7. Как отзывать и управлять ключами?



Current state:

1. Создали
2. Делаем s
3. Выставля
4. Базово п
5. Если пов
6. Вход по к
7. Как отзы
   ключи?

Кейс из жизни

Получаю VM

login: root

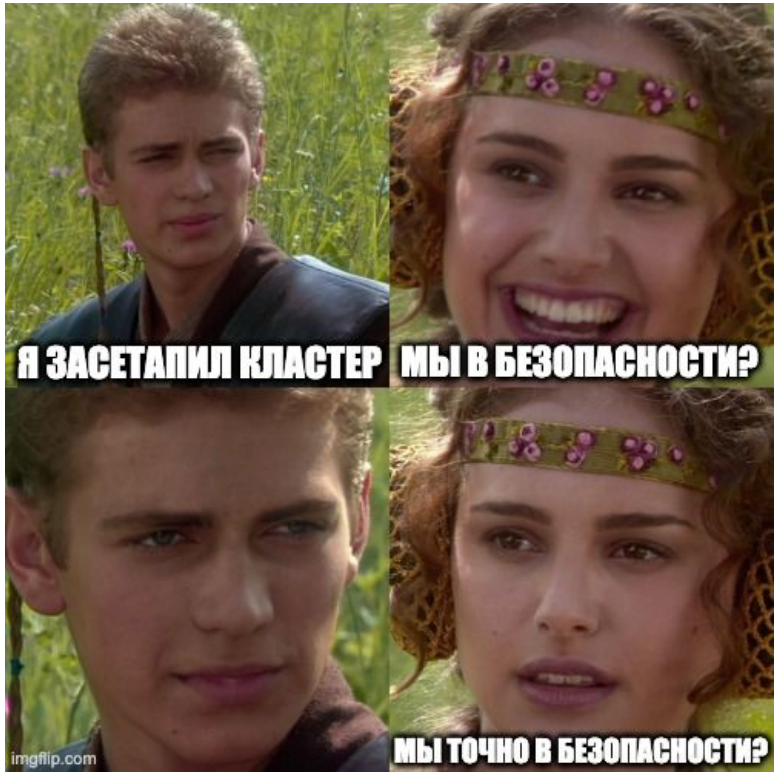
pass: qwerty12345

Operating System	Vulnerabilities	Scan Duration	
Ubuntu Linux 14.04	470	5 minutes	
Ubuntu Linux 14.04	370	5 minutes	
CentOS Linux	270	15 minutes	
Debian Linux 7.0	201	7 minutes	
Microsoft Windows Server 2008 Standard Edition SP2	98	19 minutes	
Ubuntu Linux 16.04	77	5 minutes	
Ubuntu Linux 12.04	67	10 minutes	
Microsoft Windows	42	9 minutes	
Microsoft Windows Server 2016 Standard Edition	36	8 minutes	
Microsoft Windows Server 2012 R2 Standard Edition	34	9 minutes	

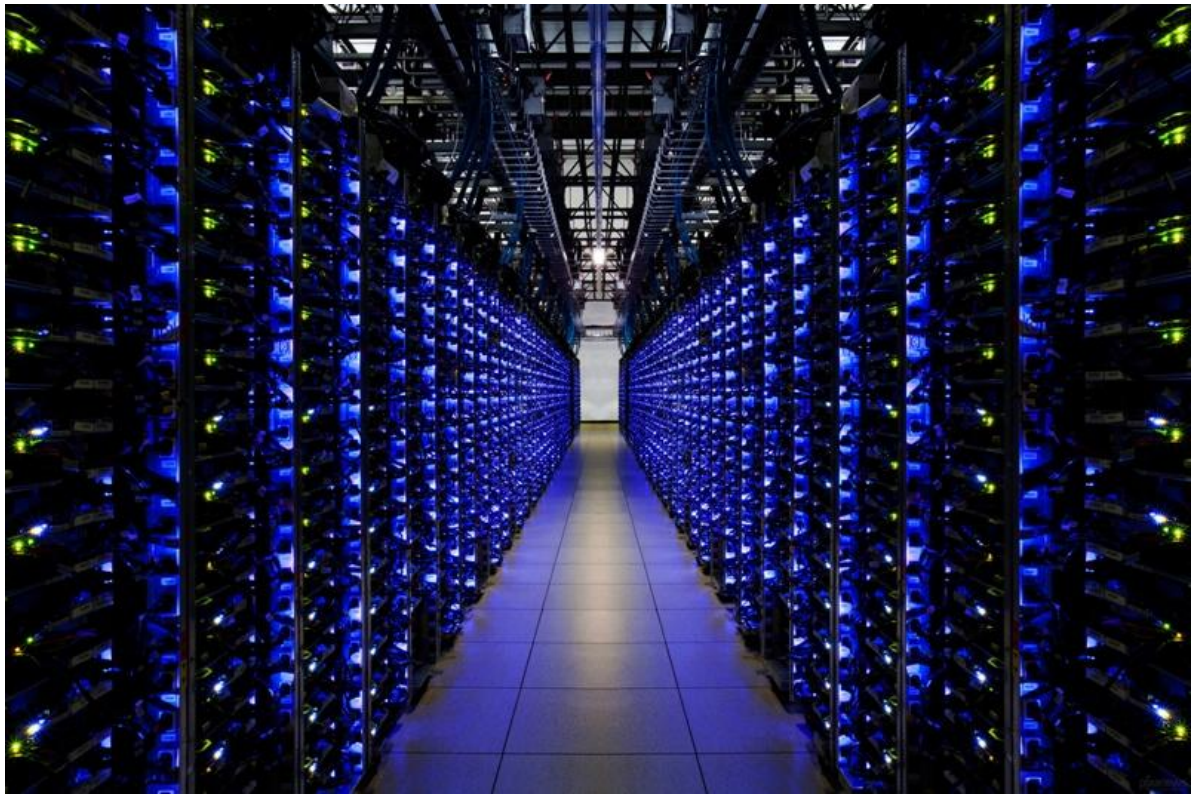
Kubernetes

- засетапить любимым способом
- …
- PROFIT!

Kubernetes


Я ЗАСЕТАПИЛ КЛАСТЕР
МЫ В БЕЗОПАСНОСТИ?
МЫ ТОЧНО В БЕЗОПАСНОСТИ?
imgflip.com

А если так?



А если так?

А если так?

А если так?

А если так?

А если так?

А если так?

Как автоматизировать пользователей?

Наивный подход:

возьмем

playbook -> 1000 servers

Как автоматизировать пользовател

Наивный подход:

возьмем

playbook -> 1000 servers

Как выдавать гранулярный доступ?

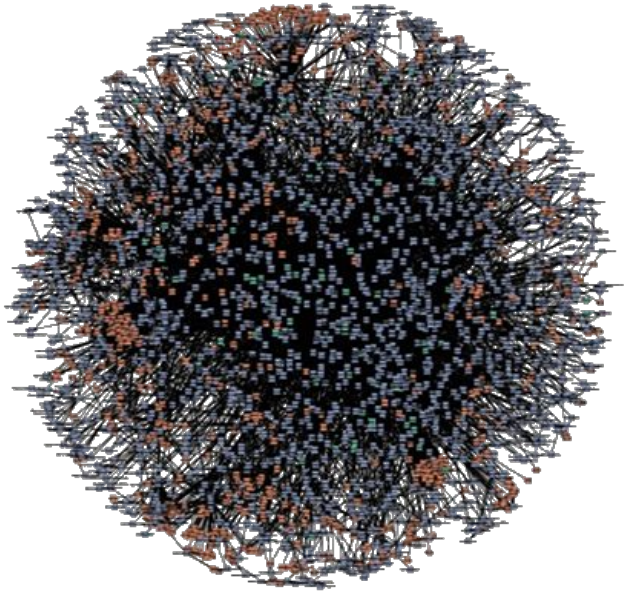
Как автоматизировать пользователей?

Чуточку лучше:

у нас есть Active Directory, возьмем sssd

Ставьте + кто осилил sssd

Плоская сеть на предприятии



amazon.com

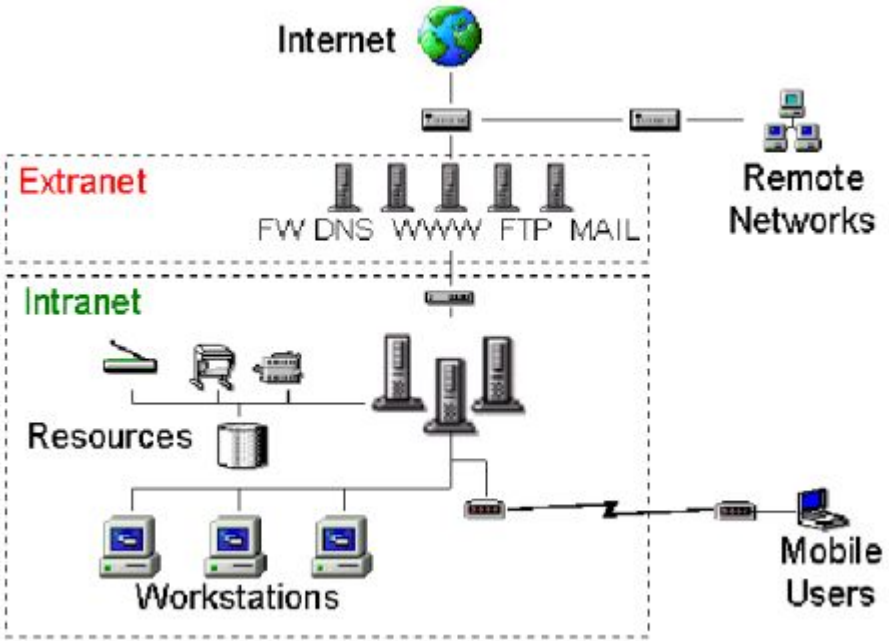
NETFLIX

А еще есть сервисы

Какие проблемы с сервисами?

Какие проблемы с сервисами?

- http сервисы торчат в интранет или интернет



Какие проблемы с сервисами?

- http сервисы торчат в интранет или интернет
- частенько из-за неправильной конфигурации сервисы для интранета начинают быть доступны напрямую из интернета

Какие проблемы с сервисами?

- http сервисы торчат в интранет или интернет
- частенько из-за неправильной конфигурации сервисы для интранета начинают быть доступны напрямую из интернета
- http (не SSL)

Какие проблемы с сервисами?

- http сервисы торчат в интранет или и
- частенько из-за неправильной конфи
  начинают быть доступны напрямую из
- http (не SSL)

Какие проблемы с сервисами?

- http сервисы торчат в интранет или интернет
- частенько из-за неправильной конфигурации сервисы для интранета начинают быть доступны напрямую из интернета
- http (не SSL)
- беспарольные (без аутентификации)

Какие проблемы с сервисами?

- http сервисы торчат в интранет или интернет
- частенько из-за неправильной конфигурации сервисы для интранета начинают быть доступны напрямую из интернета
- http (не SSL)
- беспарольные (без аутентификации)
- либо дефолтные креды admin:admin

Какие проблемы с сервисами?

- http сервисы торчат в интранет или интернет
- частенько из-за неправильной конфигурации сервисы для интранета начинают быть доступны напрямую из интернета
- http (не SSL)
- беспарольные (без аутентификации)
- либо дефолтные креды admin:admin
- с CVE (пример java log4j)

Какие проблемы с сервисами?

- http сервисы торчат в интранет или интернет
- частенько из-за неправильной конфигурации сервисы для интранета начинают быть доступны напрямую из интернета
- http (не SSL)
- беспарольные (без аутентификации)
- либо дефолтные креды admin:admin
- с CVE (пример java log4j)
- всякие дополнительные ручки не нужные (метрик - доп инфа для взломщика)

Что делать?

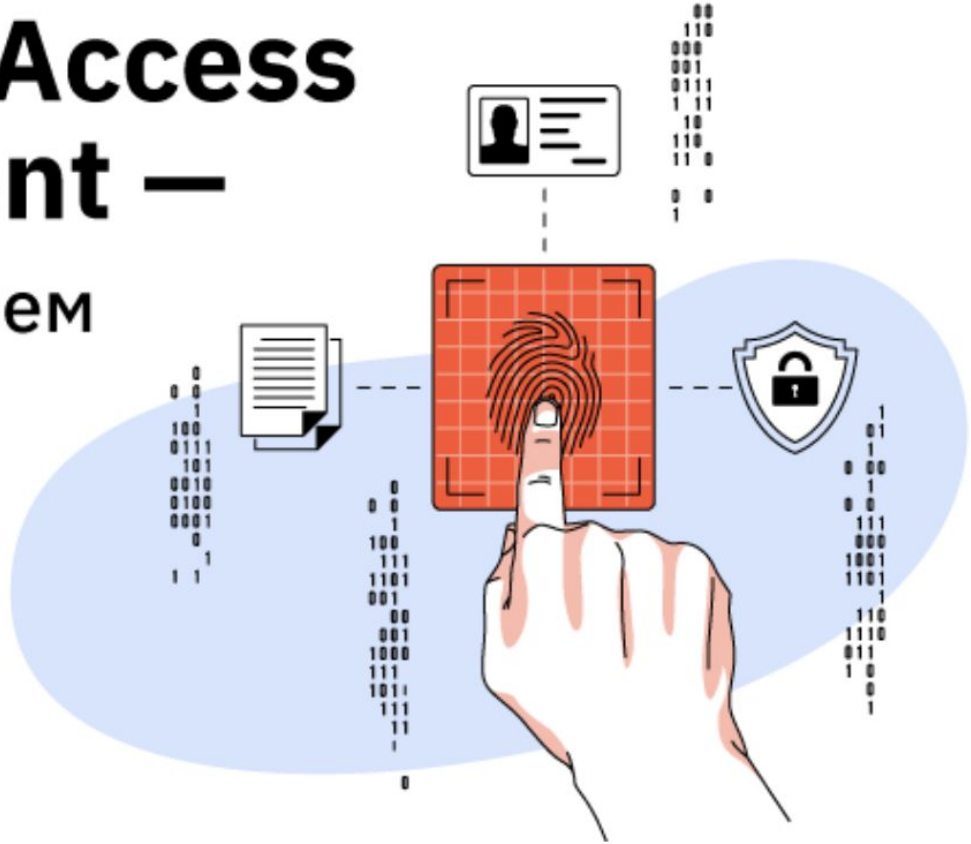
Что делать?

Решение есть

Решение есть - PAM

Privileged Access Management —

когда не доверяем никому



Что такое PAM и с чем едят?

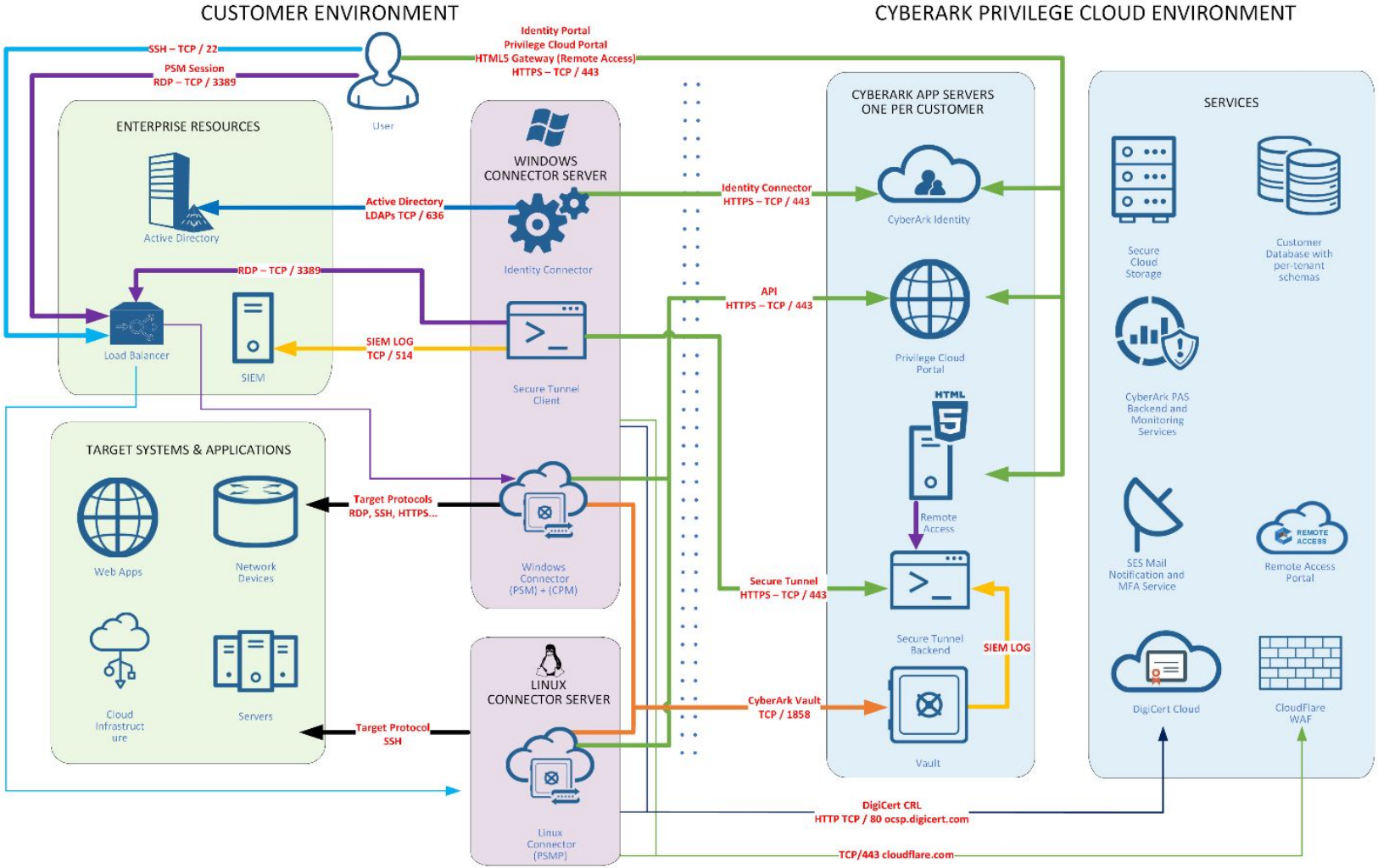
программный комплекс, который обеспечивает безопасный доступ к системам.

В первую очередь - административный

Классика PAM

CyberArk - что-то на энтерпрайзном

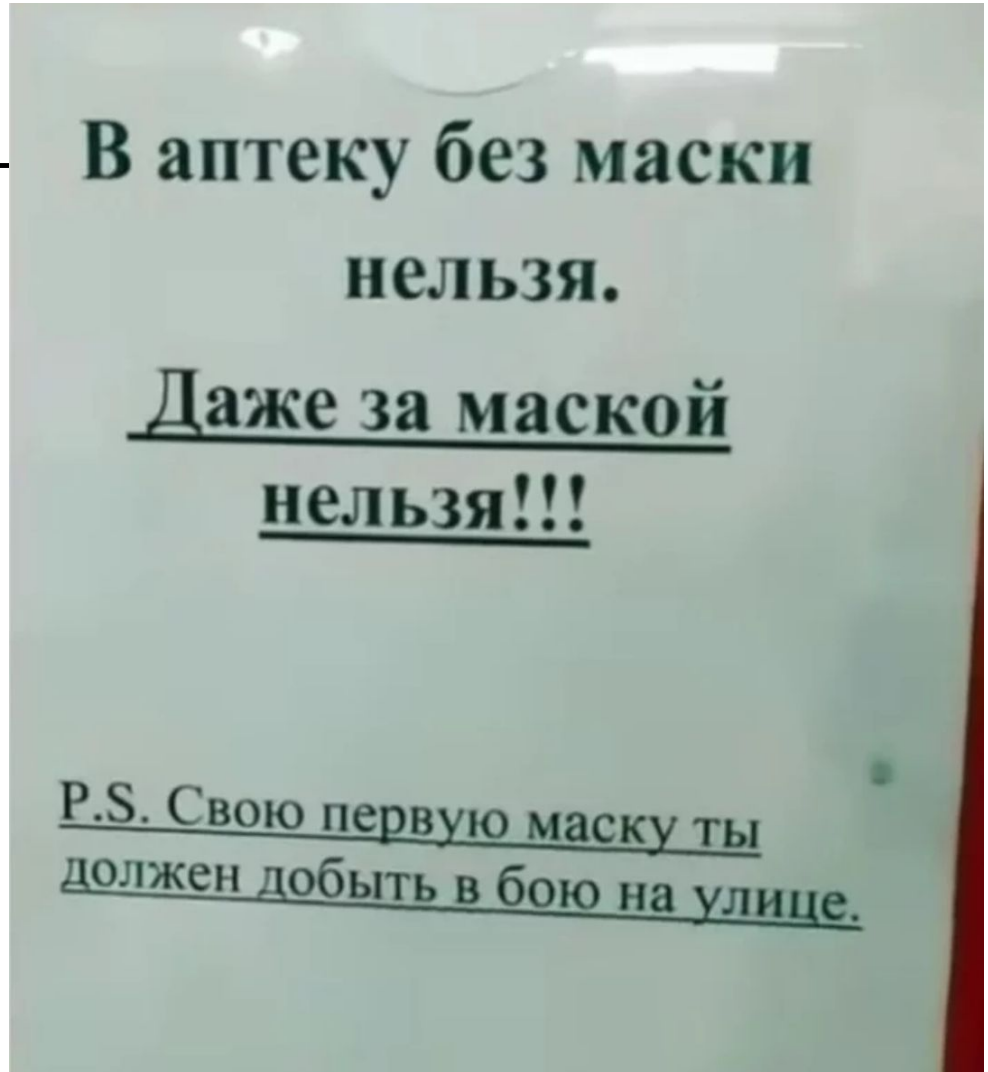
КиберКовчег?


CUSTOMER ENVIRONMENT
CYBERARK PRIVILEGE CLOUD ENVIRONMENT
SSH – TCP / 22
PSM Session
RDP – TCP / 3389
Identity Portal
Privilege Cloud Portal
HTML5 Gateway (Remote Access)
HTTPS – TCP / 443
User
ENTERPRISE RESOURCES
Active Directory
Load Balancer
SIEM
WINDOWS CONNECTOR SERVER
Identity Connector
Secure Tunnel Client
Windows Connector (PSM) + (CPM)
Active Directory
LDAPs TCP / 636
RDP – TCP / 3389
SIEM LOG
TCP / 514
TARGET SYSTEMS & APPLICATIONS
Web Apps
Network Devices
Cloud Infrastructure
Servers
Target Protocols
RDP, SSH, HTTPS...
LINUX CONNECTOR SERVER
Linux Connector (PSMP)
Target Protocol
SSH
CYBERARK APP SERVERS ONE PER CUSTOMER
CyberArk Identity
Privilege Cloud Portal
HTML
Remote Access
Secure Tunnel Backend
Vault
Identity Connector
HTTPS – TCP / 443
API
HTTPS – TCP / 443
Secure Tunnel
HTTPS – TCP / 443
SIEM LOG
CyberArk Vault
TCP / 1858
SERVICES
Secure Cloud Storage
Customer Database with per-tenant schemas
CyberArk PAS Backend and Monitoring Services
SES Mail Notification and MFA Service
REMOTE ACCESS
Remote Access Portal
DigiCert Cloud
CloudFlare WAF
DigiCert CRL
HTTP TCP / 80 ocsp.digicert.com
TCP/443 cloudflare.com

Что должно быть в хорошем PAM?

Что должно быть в хорош

- Контроль доступа



Что должно быть в хорошем PAM?

- Контроль доступа
- Аудит

Что должно быть в хорошем PAM?

- Контроль доступа
- Аудит
- Запрос доступа

Что должно быть в хорошем PAM?

- Контроль доступа
- Аудит
- Запрос доступа
- Интеграция с каталогами пользователей (SSO, LDAP)

Что должно быть в хорош

- Контроль доступа
- Аудит
- Запрос доступа
- Интеграция с каталогами поль
- 2FA/MFA

Что должно быть в хор

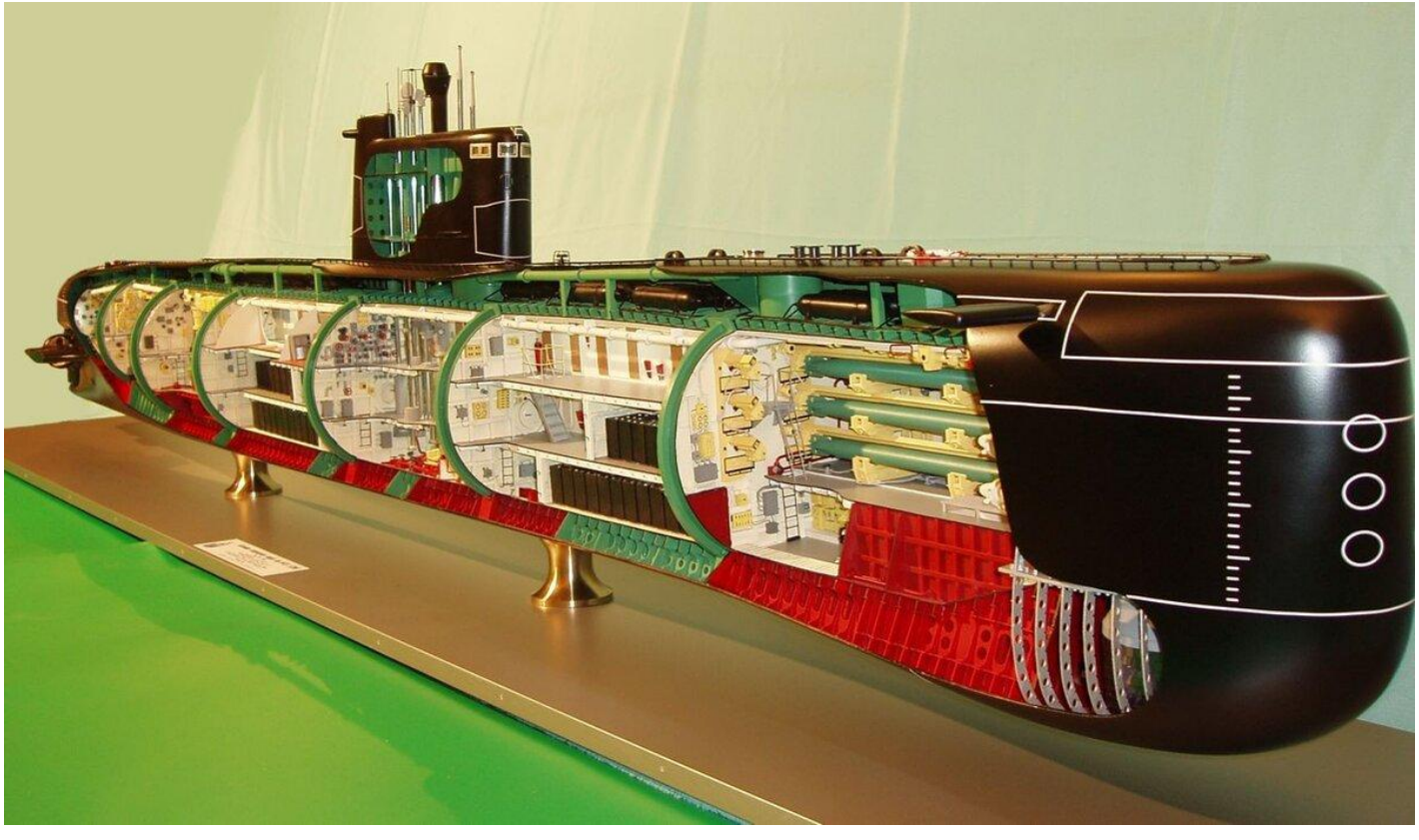
- Контроль доступа
- Аудит
- Запрос доступа
- Интеграция с каталогами п
- 2FA/MFA
- Zero Trust Network Access

Что должно быть в хорошем PAM?

- Контроль доступа
- Аудит
- Запрос доступа
- Интеграция с каталогами пользователей (SSO, LDAP)
- 2FA/MFA
- Zero Trust Network Access
- Short living keys

Цитадель - периметры безопасности

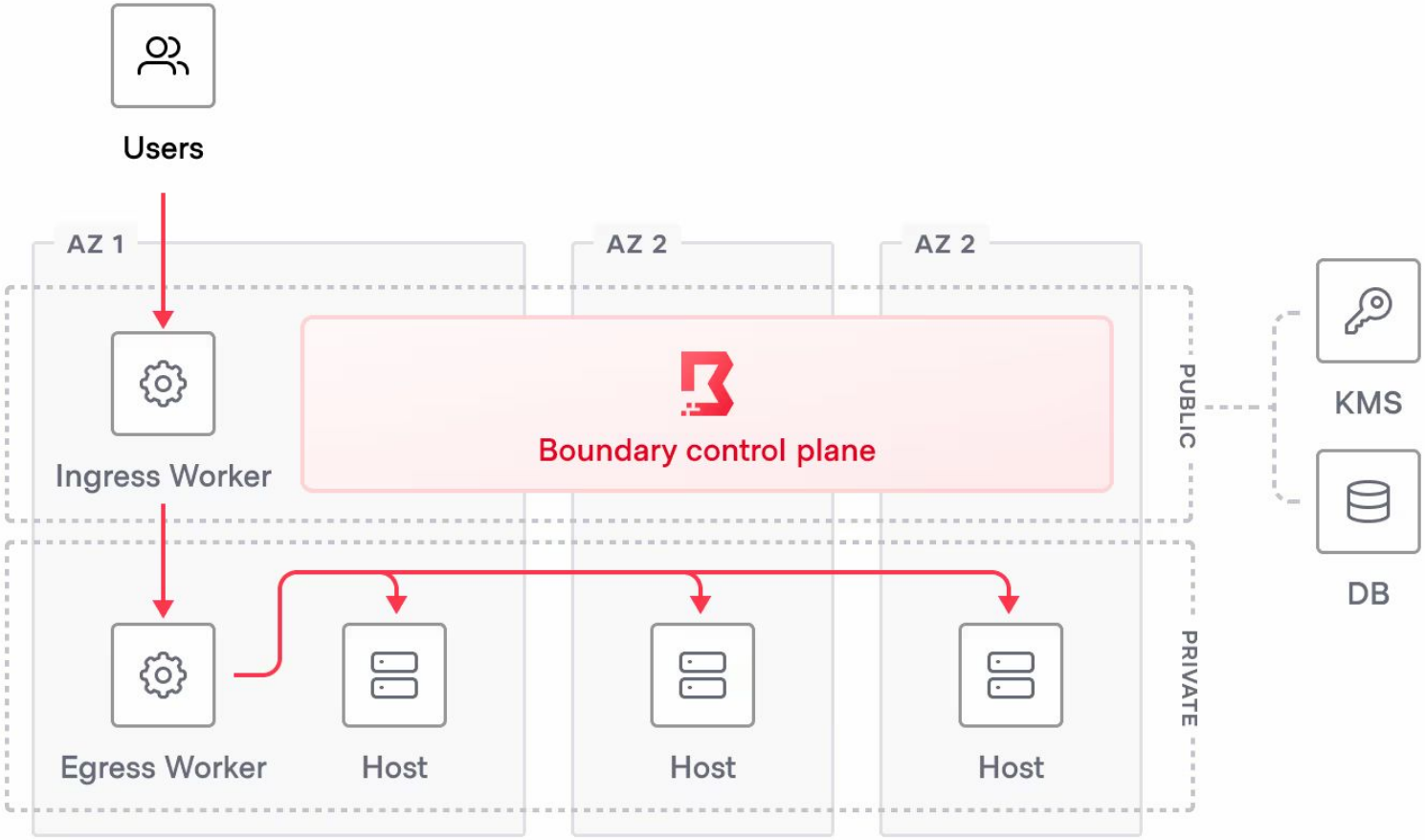
Ячеистая инфраструктура



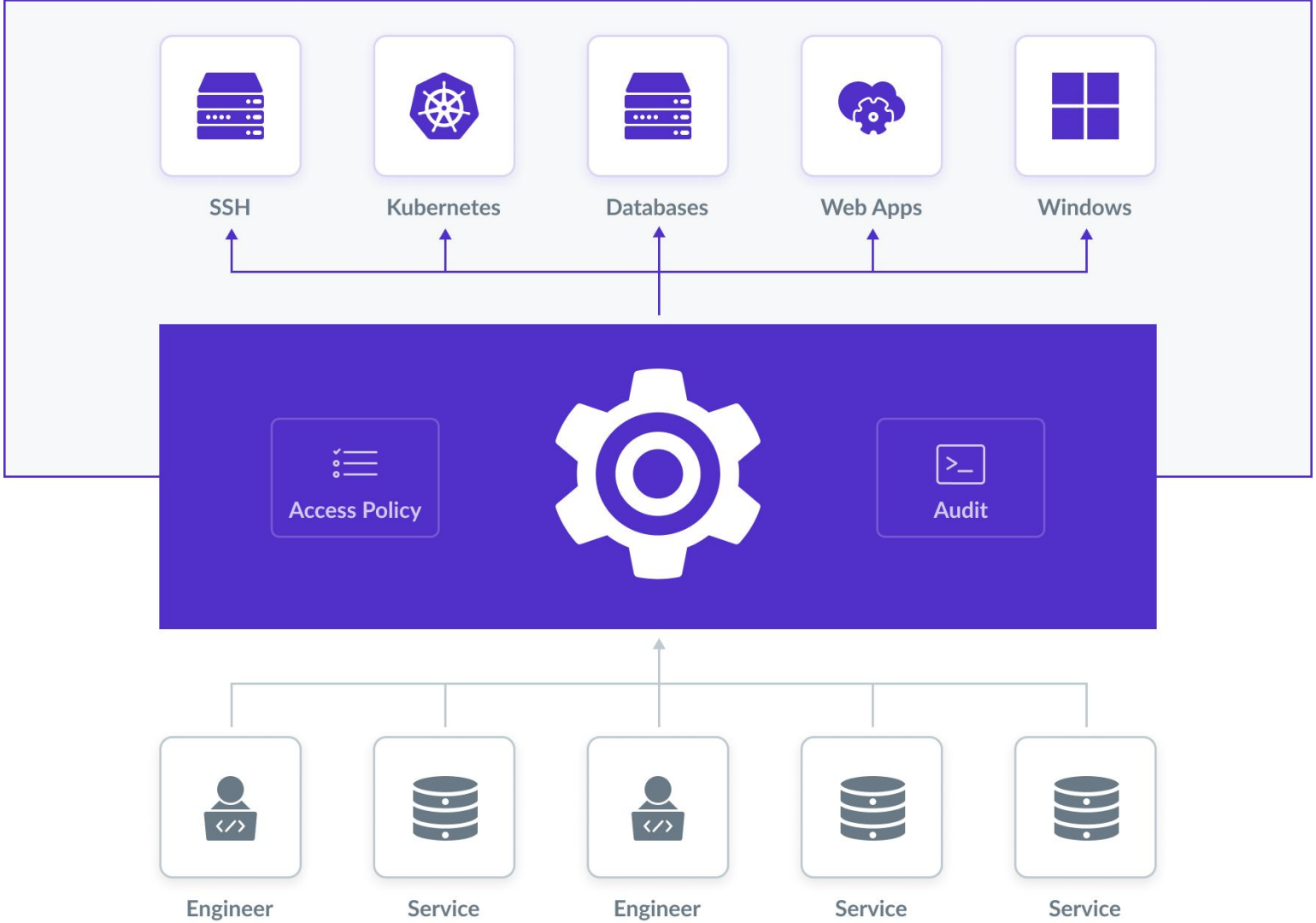
Какие решения есть на рынке?

HashiCorp

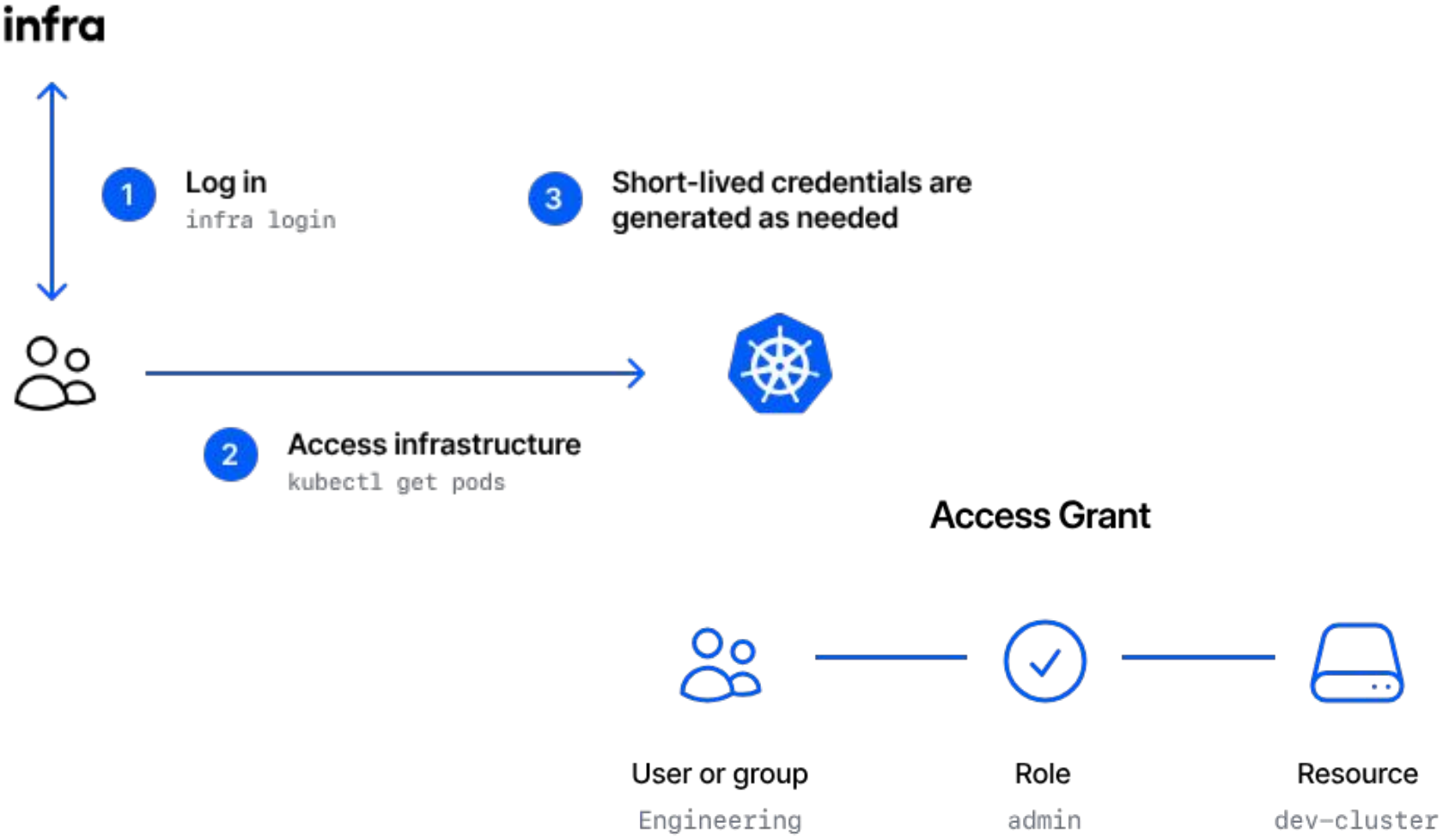
Boundary


Users
AZ 1
AZ 2
AZ 2
Ingress Worker
Boundary control plane
PUBLIC
KMS
DB
Egress Worker
Host
Host
Host
PRIVATE


TELEPORT


SSH
Kubernetes
Databases
Web Apps
Windows
Access Policy
Audit
Engineer
Service
Engineer
Service
Service

Infra provides authentication and access management to servers, clusters, and databases.


infra
1
Log in
infra login
3
Short-lived credentials are generated as needed
2
Access infrastructure
kubectl get pods
Access Grant
User or group
Engineering
Role
admin
Resource
dev-cluster


FUDO
PAM

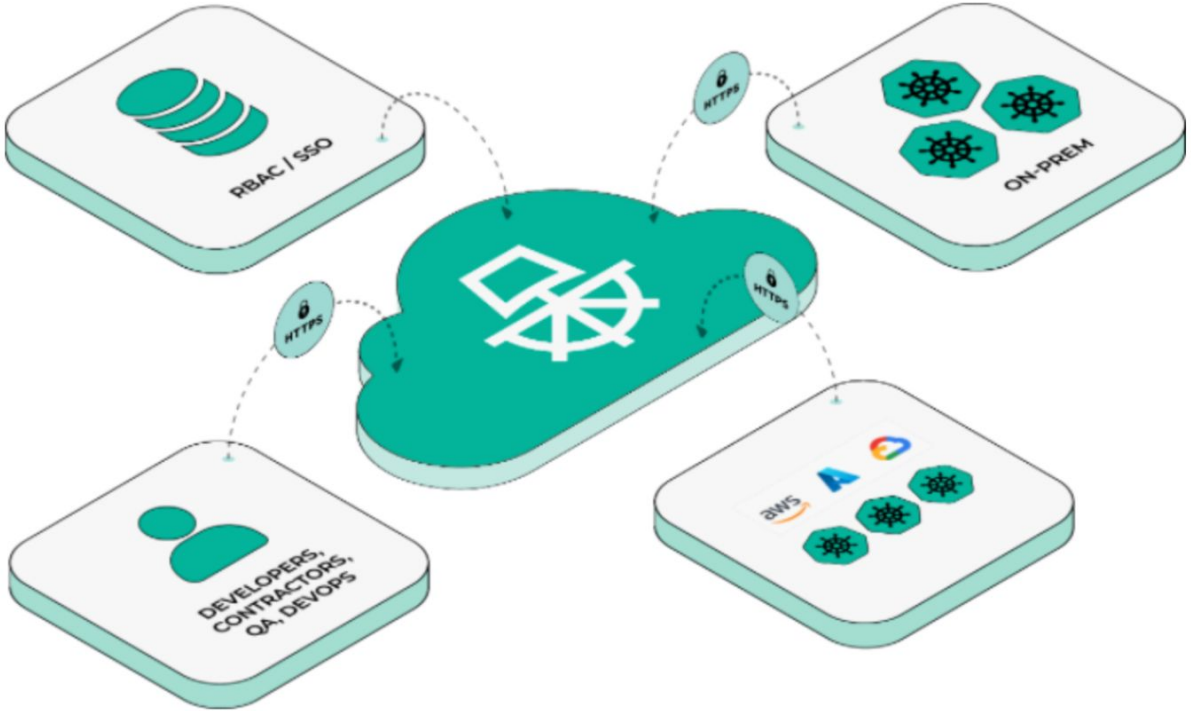
ПРИНЦИП РАБОТЫ FUDO PAM

FUDO | PAM

www.fudosecurity.com

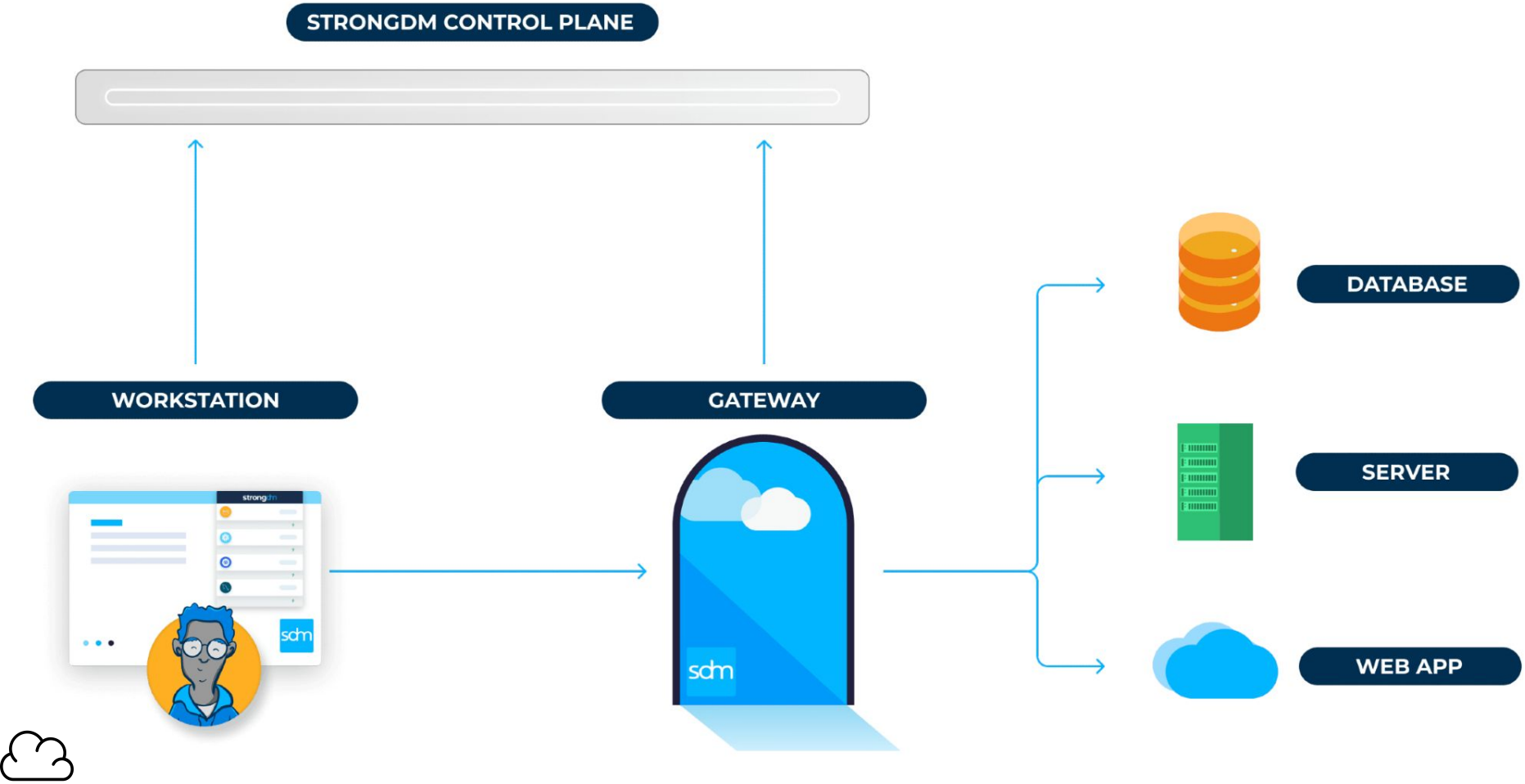
FUDO SECURITY

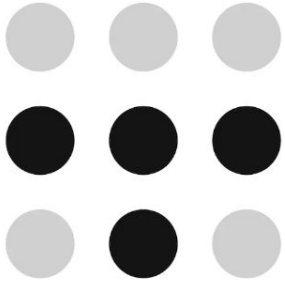
PARALUS



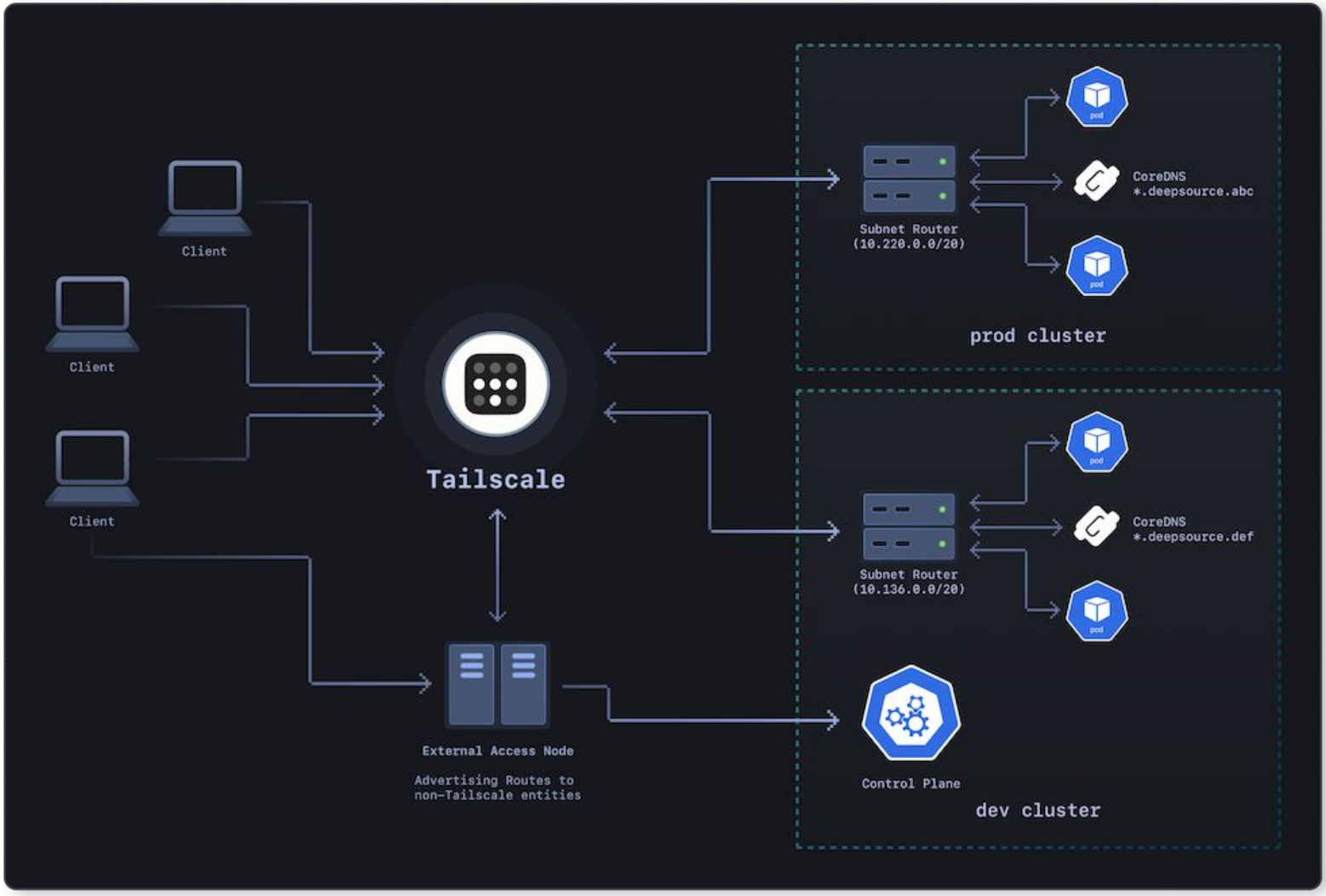
Zero trust Kubernetes with zero friction


strongdm


STRONGDM CONTROL PLANE
WORKSTATION
GATEWAY
DATABASE
SERVER
WEB APP
sdm
sdm

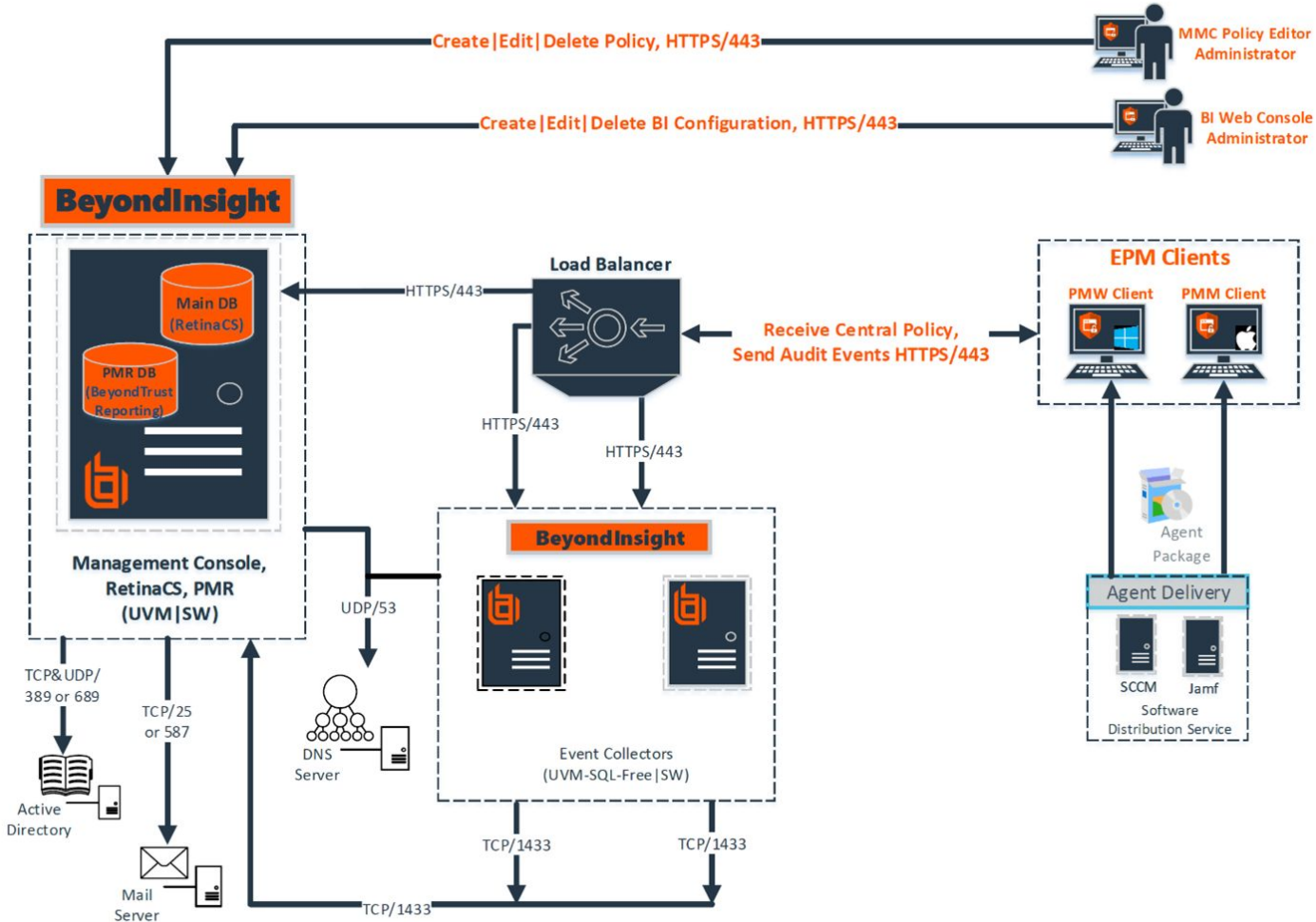


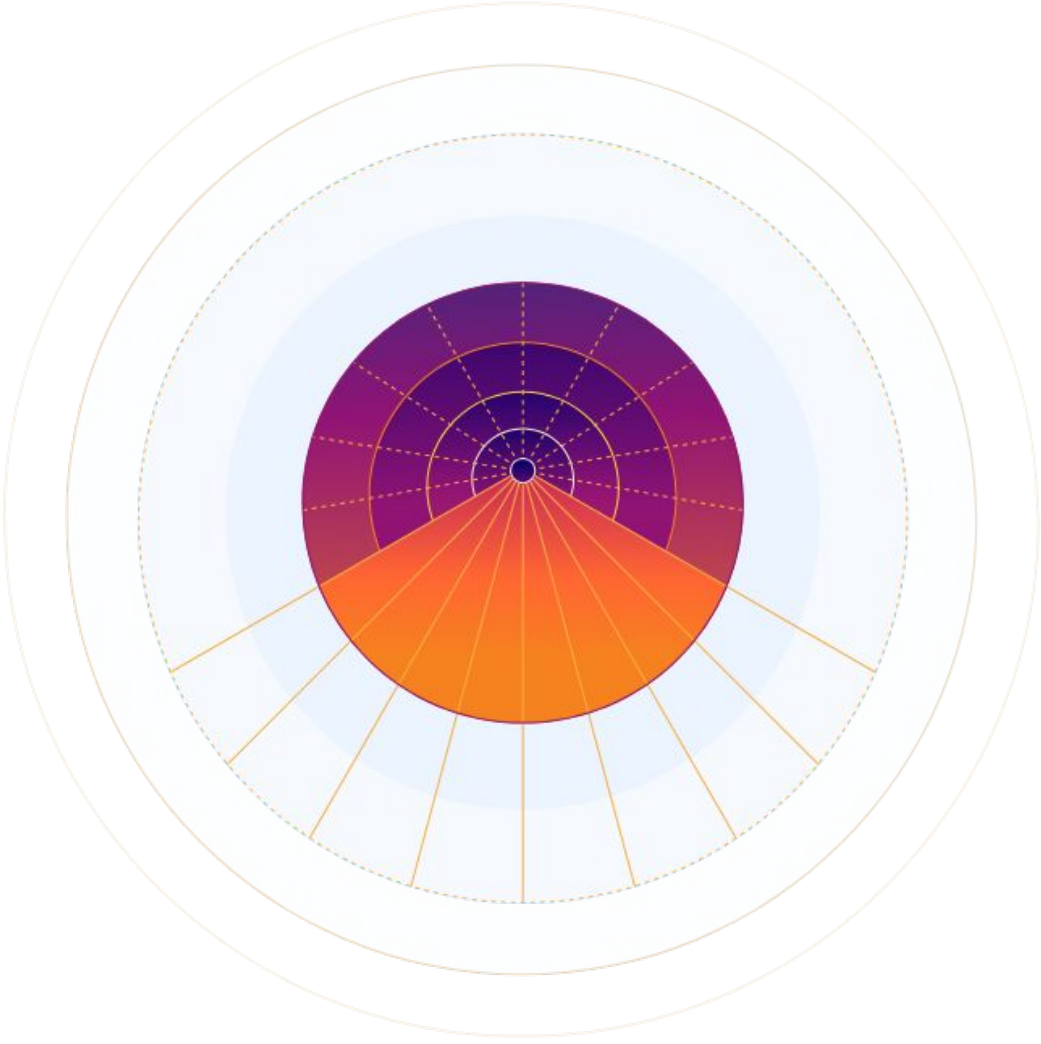
tailscale

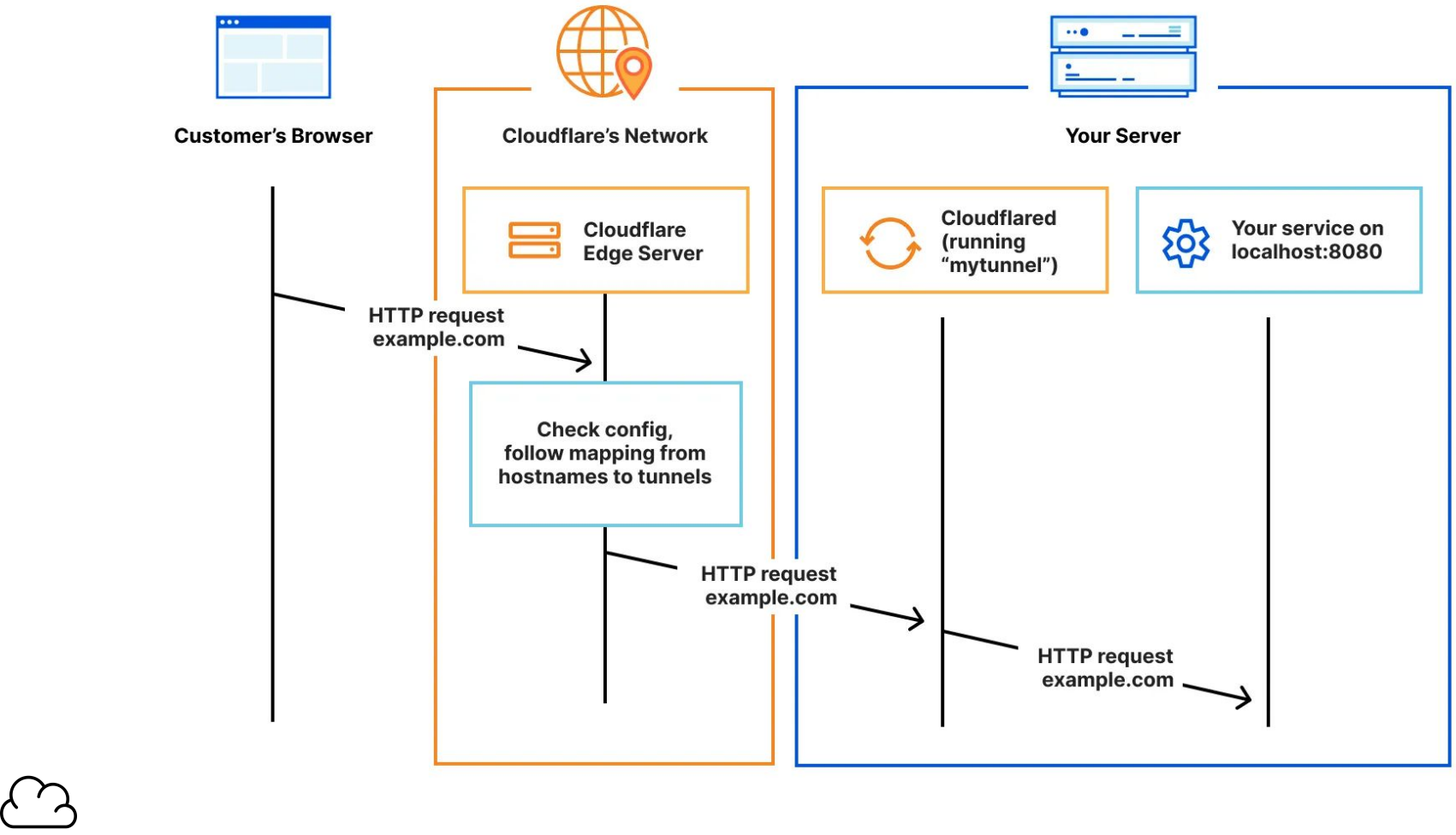

Client
Client
Client
Tailscale
External Access Node
Advertising Routes to
non-Tailscale entities
Subnet Router
(10.220.0.0/20)
pod
CoreDNS
*.deepsource.abc
pod
prod cluster
Subnet Router
(10.136.0.0/20)
pod
CoreDNS
*.deepsource.def
pod
Control Plane
dev cluster


BeyondTrust

Endpoint Privilege Management – BeyondInsight Architecture






Customer's Browser
Cloudflare's Network
Your Server
Cloudflare Edge Server
Cloudflared (running "mytunnel")
Your service on localhost:8080
HTTP request example.com
Check config, follow mapping from hostnames to tunnels
HTTP request example.com
HTTP request example.com

	Boundary			FUDO | PAM		strongdm		BeyondTrust	
OSS or proprietary	CE+EE	CE+EE	OSS	Prop	OSS	Prop	Prop	Prop	Prop
Free or paid	CE+EE	CE+EE	Free	CE и EE	Free	Paid	Paid	Paid	Paid
Support	EE	EE	✗	EE	Slack	✓	✓	✓	✓
ssh	✓	✓	✓	✓	✗	✓	✓	?	✓
k8s	✓	✓	✓	EE	✓	✓	✗	?	✗
DB	✓	✓	✗	EE	✗	✓	✓	?	✗
RDP	✓	✓	✗	✓	✗	✓	✓	?	✓ ✗
http	?	✓	✗	EE	✗	✓	✓	?	✓
cloud api	?	?	✗	EE	✗	?	✓	✓	✗

									
audit									
2FA/MFA	?	SSO			SSO				
LDAP & etc. in free version		EE	SSO	EE	SSO				
FIPS, PCI DSS, HIPAA		EE							
setup complexity									
agent/agentless	EE								
Local cli									
Sessions record (ssh+k8s)	EE			EE					
Access request workflow	EE								

Останавливаемся на телепорте

бесплатно - opensource, но нет части жизненно необходимого функционала:

- синхронизация пользователей
- request workflow

платно - очень дорого (примерно 10000 евро на 10 пользователей за год)

Останавливаемся на телепорте

бесплатно - opensource, но нет части жизненно необходимого функционала:

- синхронизация пользователей
- request workflow

платно - очень дорого (примерно 10000 евро на 10 пользователей за год)

- зато FIPS! PCI DSS и прочее

Почему нет нормального продукта на рынке?

Почему нет нормального продукта на рынке?

- дорого

Почему нет нормального продукта на рынке?

- дорого
- сервисы, которые надо защищать очень разные:
  - kubernetes
  - ssh
  - http
  - БД
  - межсервисная аутентификация
  - RDP

Что видим сейчас:

Компании берут Teleport CE и допиливают под свои нужды

Что видим сейчас:

Компании берут Teleport CE и допиливают под свои нужды

Есть и минусы по опыту использования:

- агентная архитектура, построенная на реверс туннелях

Что видим сейчас:

Компании берут Teleport CE и допиливают под свои нужды

Есть и минусы по опыту использования:

- Агентная архитектура, построенная на реверс туннелях
- При потере соединений - кластер сам себя DDoSит в попытках переподключиться

Что видим сейчас:

Компании берут Teleport CE и допиливают под свои нужды

Есть и минусы по опыту использования:

- Агентная архитектура, построенная на реверс туннелях
- При потере соединений - кластер сам себя DDoSит в попытках переподключиться
- Еще есть баги с количеством ролей

Что видим сейчас:

Компании берут Teleport CE и допиливают под свои нужды

Есть и минусы по опыту использования:

- Агентная архитектура, построенная на реверс туннелях
- При потере соединений - кластер сам себя DDoSит в попытках переподключиться
- Еще есть баги с количеством ролей. Алгоритм их перебора обладает линейной сложностью

Что видим сейчас:

Компании берут Teleport CE и допиливают под свои нужды

Есть и минусы по опыту использования:

- Агентная архитектура, построенная на реверс туннелях
- При потере соединений - кластер сам себя DDoSит в попытках переподключиться
- Еще есть баги с количеством ролей. Алгоритм их перебора обладает линейной сложностью
- Соответственно чем их больше - тем дольше подключается агент

Что видим сейчас:

Компании берут Teleport CE и допиливают под свои нужды

Есть и минусы по опыту использования:

- Агентная архитектура, построенная на реверс туннелях
- При потере соединений - кластер сам себя DDoSит в попытках переподключиться
- Еще есть баги с количеством ролей. Алгоритм их перебора обладает линейной сложностью
- Соответственно чем их больше - тем дольше подключается агент
- Менеджмент ролей очень непрозрачен

Выводы

- Сетевая сегментация не дает нужного уровня безопасности

Выводы

- Сетевая сегментация не дает нужного уровня безопасности
- PAM дает гранулярный и контролируемый доступ

Выводы

- Сетевая сегментация не дает нужного уровня безопасности
- PAM дает гранулярный и контролируемый доступ
- Надо делать безопасно сразу, иначе потом дорого

Выводы

- Сетевая сегментация не дает нужного уровня безопасности
- PAM дает гранулярный и контролируемый доступ
- Надо делать безопасно сразу, иначе потом дорого
- и больно)

Ссылки

Telegram группа

teleport