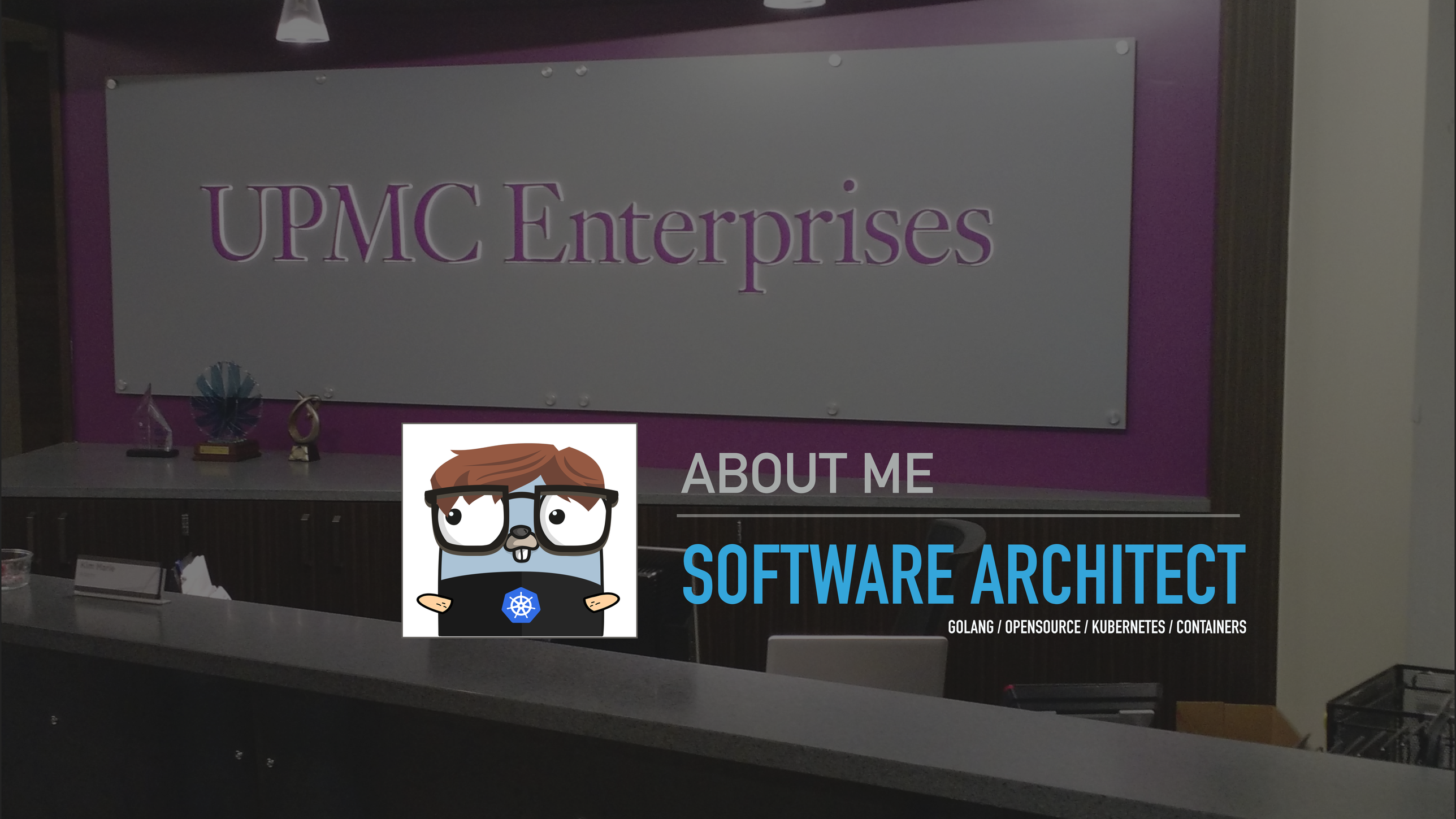
KubeCon

North America 2017

HYBRID-CLOUD, HIPPA COMPLIANT ENTERPRISE WITH KUBERNETES

STEVE SLOKA



ABOUT ME

SOFTWARE ARCHITECT

GOLANG / OPENSOURCE / KUBERNETES / CONTAINERS

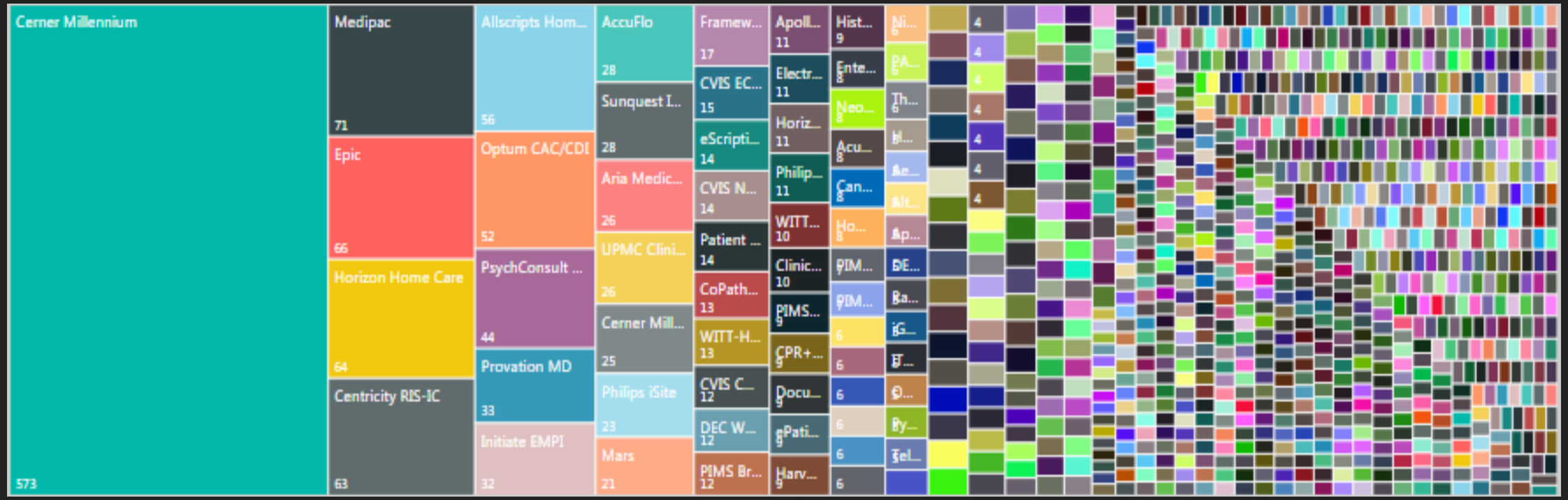
UNIVERSITY OF PITTSBURGH MEDICAL CENTER

- $16 billion integrated global nonprofit health enterprise
- 80k employees
- > 30 hospitals
- 3.2 Million member health insurance division
- “Other Stuff”

https://en.wikipedia.org/wiki/University_of_Pittsburgh_Medical_Center

CLINICAL DATA @ UPMC

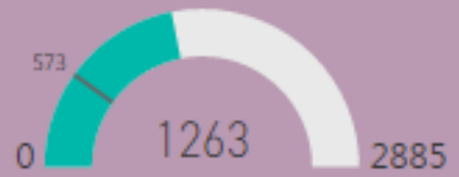
UPMC (CLINICAL) DATA SOURCE INVENTORY



Total Number of Apps

1102

Data Domains of Top 20 Apps



Application Name	Count of Application Name
Cerner Millennium	573
Medipac	71
Epic	66
Horizon Home Care	64
Centricity RIS-IC	63
Allscripts Homecare	56
Total	**1263**

WHAT IS HIPAA?

- HIPAA = **H**ealth **I**nsurance **P**ortability and **A**ccountability **A**ct
- Prohibit the disclosure or misuse of information about private individuals
- **Types of Data?**
  - Social Security Numbers
  - Medical Record Numbers (MRN)
  - Patient Name
  - (Anything that can describe a patient specifically)

WHY CREATE HIPAA?


`STANDARDS`

HIPAA RULES

- Encryption at REST
- Encryption in TRANSIT
- Auditing to the user
- BAA (Business Associate Agreement)

ON-PREMISES

ON-PREMISES

- **Kubernetes Infrastructure**
  - Red Hat Atomic
  - CoreOS Tectonic
- **Storage**
  - NFS
  - Local Storage
- **Load Balancers**
  - F5 ––> NodePorts && Ingress

ON-PREMISES

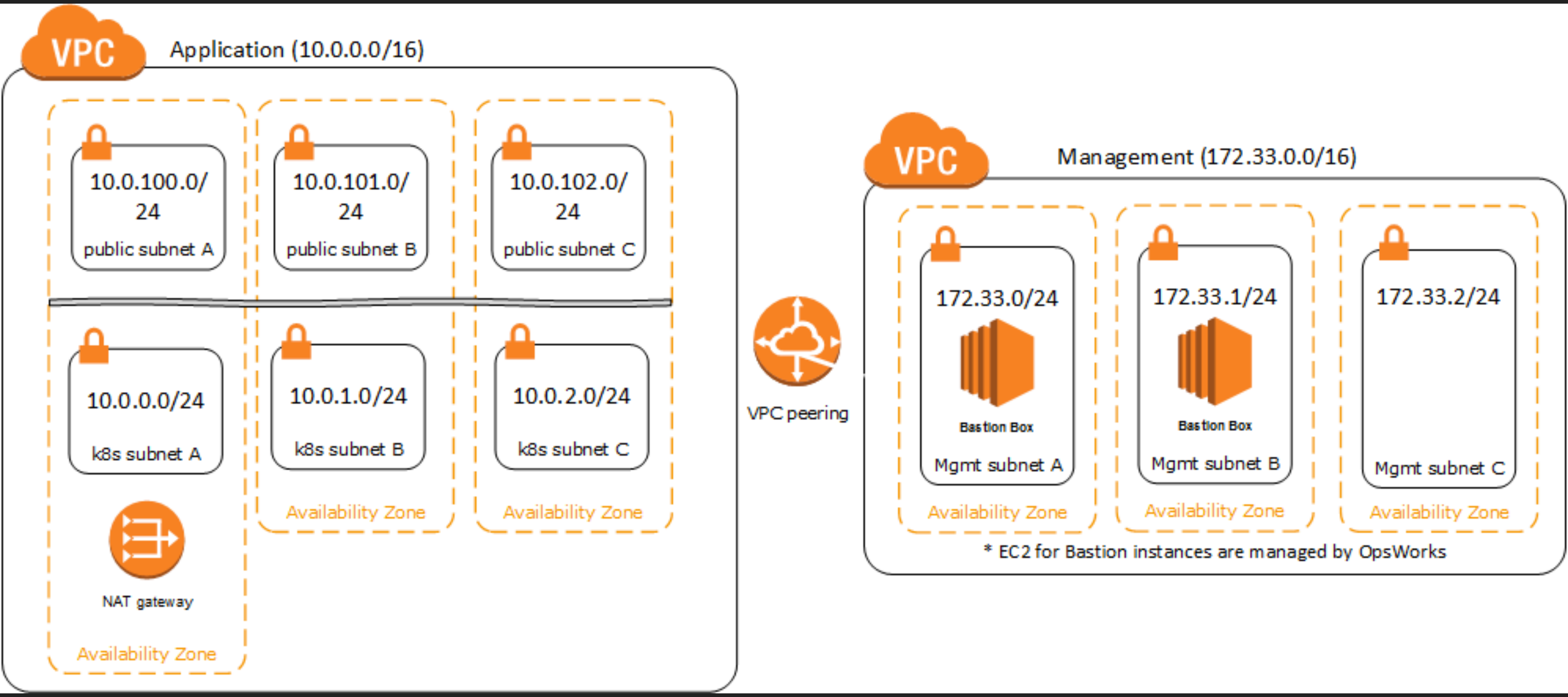
- Workloads
  - CI/CD (Gitlab Runners / Jenkins Workers)
  - Local “agents”
    - Data Collection
    - Data Proxies

ON-PREMISES IS HARD(ER)

PUBLIC CLOUD

CLOUD INFRASTRUCTURE

- Amazon Web Services (AWS)
- Single Region / Multi-AZ
- Multiple worker Auto-scaling Groups (ASG)
- CloudFormation + CoreOS (Container Linux)
- ECR Docker Registry
- Classic ELB
- VPN to OnPrem



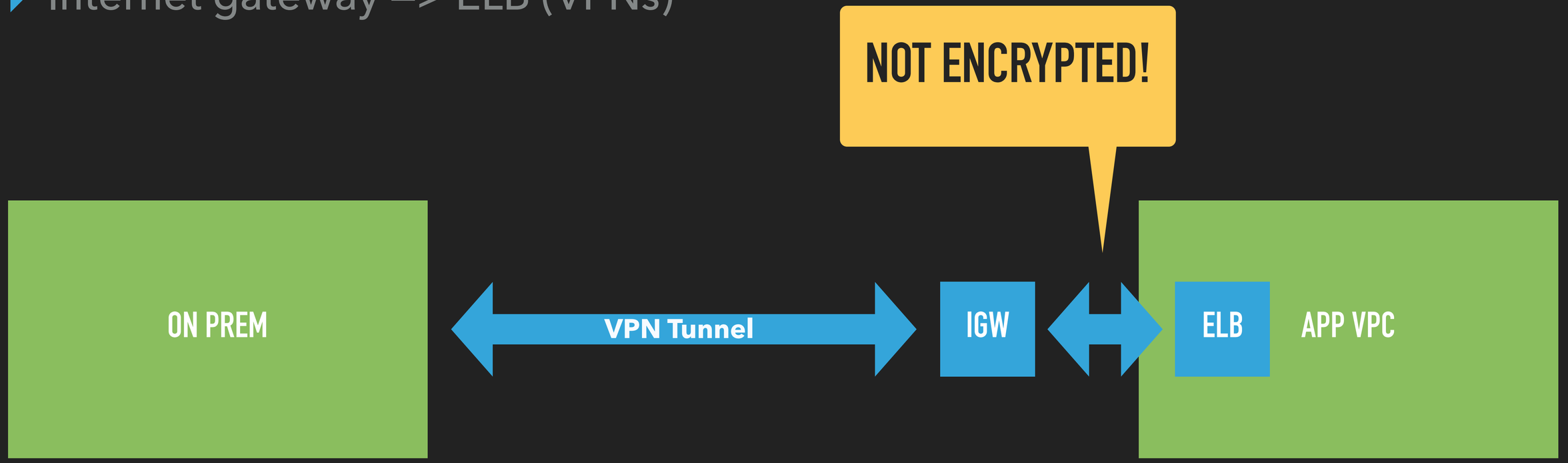
https://github.com/upmc-enterprises/kubernetes-on-aws

AWS HIPPA COMPLIANT OFFERINGS

- Amazon API Gateway excluding the use of Amazon API Gateway caching
- Amazon Aurora [MySQL, PostgreSQL]
- AWS Batch
- Amazon CloudFront [including Lambda@Edge]
- AWS CloudHSM
- Amazon CloudWatch Logs
- Amazon Cognito
- Amazon Connect
- AWS Database Migration Service
- AWS Direct Connect
- AWS Directory Services excluding Simple AD and AD Connector
- Amazon DynamoDB
- Amazon EC2 Container Service (ECS)
- Amazon EC2 Systems Manager
- Amazon ElastiCache
- Amazon Elastic Block Store (Amazon EBS)
- Amazon Elastic Compute Cloud (Amazon EC2)
- Elastic Load Balancing
- Amazon Elastic MapReduce (Amazon EMR)
- Amazon Glacier
- Amazon Inspector
- AWS Key Management Service
- Amazon Kinesis Streams
- AWS Lambda
- Amazon Redshift
- Amazon Relational Database Service (Amazon RDS) [SQL Server, MySQL, Oracle, PostgreSQL, and MariaDB engines only]
- Amazon Route 53
- AWS Shield [Standard and Advanced]
- Amazon Simple Notification Service (SNS)
- Amazon Simple Queue Service (SQS)
- Amazon Simple Storage Service (Amazon S3) [including S3 Transfer Acceleration]
- AWS Snowball
- AWS Snowball Edge
- AWS Snowmobile
- AWS Storage Gateway
- Amazon Virtual Private Cloud (VPC)
- AWS Web Application Firewall (WAF)
- Amazon WorkDocs
- Amazon WorkSpaces

NOT EVERYTHING IS COMPLIANT!

- New Services
- Internet gateway –> ELB (VPNs)



AWS TO THE RESCUE!

- Mike Kuentz - Senior Solutions Architect
  - @mkuentz
  - kuentzm@amazon.com

K8S WORKLOADS

STATELESS APPLICATIONS

STATELESS APPLICATIONS

- Easy-Peesy-Lemon-Squeezy
  - Self-contained
  - No storage
  - Dependencies are outside scope of `this application`
  - Easily scheduled / scaled
- Implemented via Kubernetes Deployments
- kubectl scale deployment elastic –replicas=5

STATEFUL APPLICATIONS

STATEFUL APPLICATIONS STRUGGLES

- How manage persistent storage?
- Resize/Upgrade
- Reconfigure - templating
- Backup - handle automatically

STATEFUL APPLICATIONS IMPLEMENTATION

- Statefulsets
  - Allow for persistent storage replicas to have an identity
  - One Persistent Volume per Claim

THAT'S ME RIGHT?

An Operator is an application-specific controller that extends the Kubernetes API to create, configure and manage instances of complex stateful applications on behalf of a Kubernetes user.

CoreOS

THAT'S ME RIGHT?

Make it work like a cloud provided offering.

Steve Sloka

ELASTIC-OPERATOR

https://github.com/upmc-enterprises/elasticsearch-operator

ELASTICSEARCH OPERATOR

- Mimic Cloud Offerings
- Full TLS
  - Automatic certificate generation
  - Encrypted EBS Volumes
  - Communication TLS (SearchGuard*)
- Span availability zones in AWS (Creation & Scaling)
- Snapshots to S3
- Deploy Add-ons Automatically
  - Kibana / Cerebro

* http://floragunn.com/searchguard

THERE'S SOME WORK TO DO

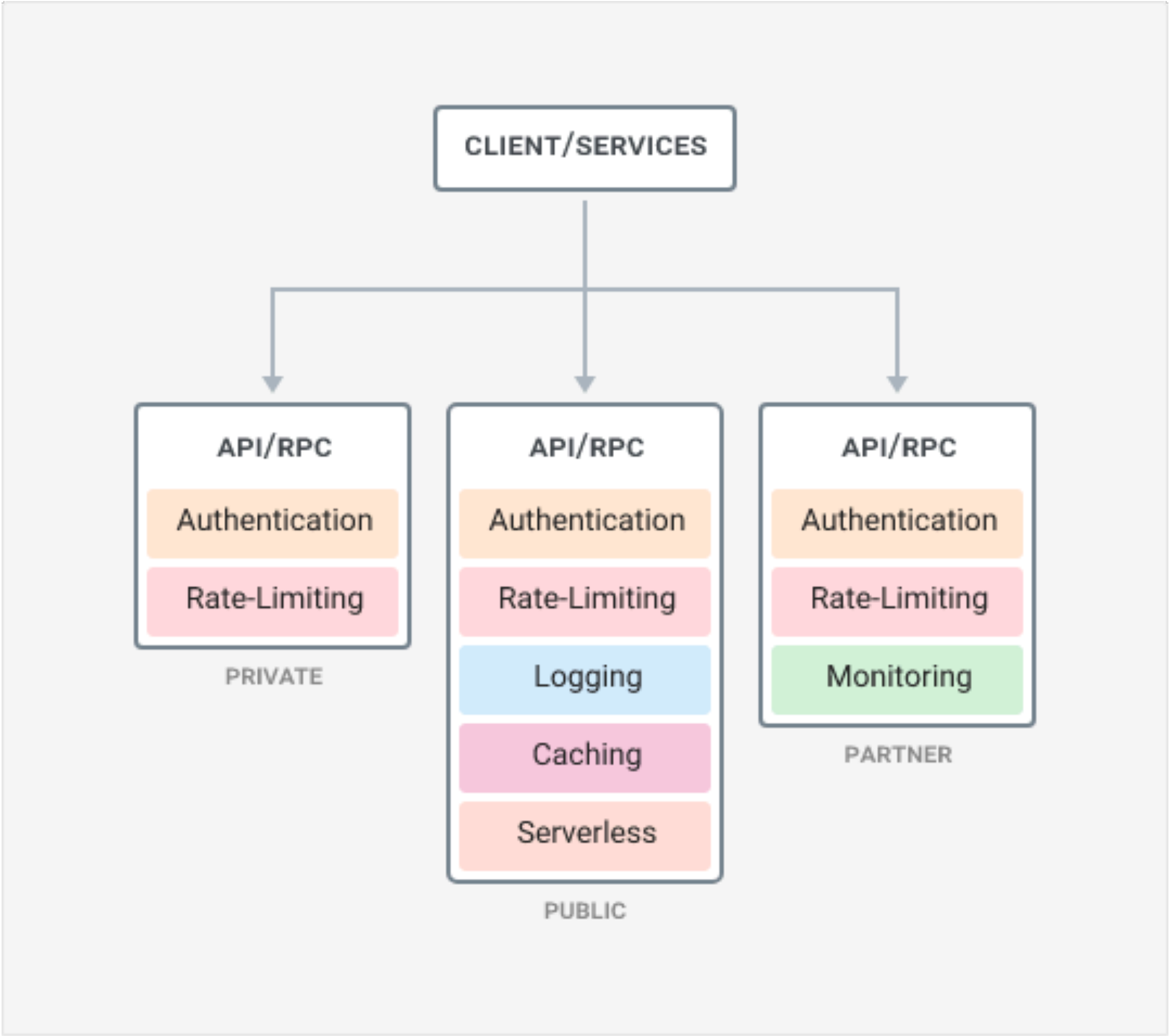
- Shard / Zone Allocation
- Elastic cluster status
- Rolling restarts
- Upgrades

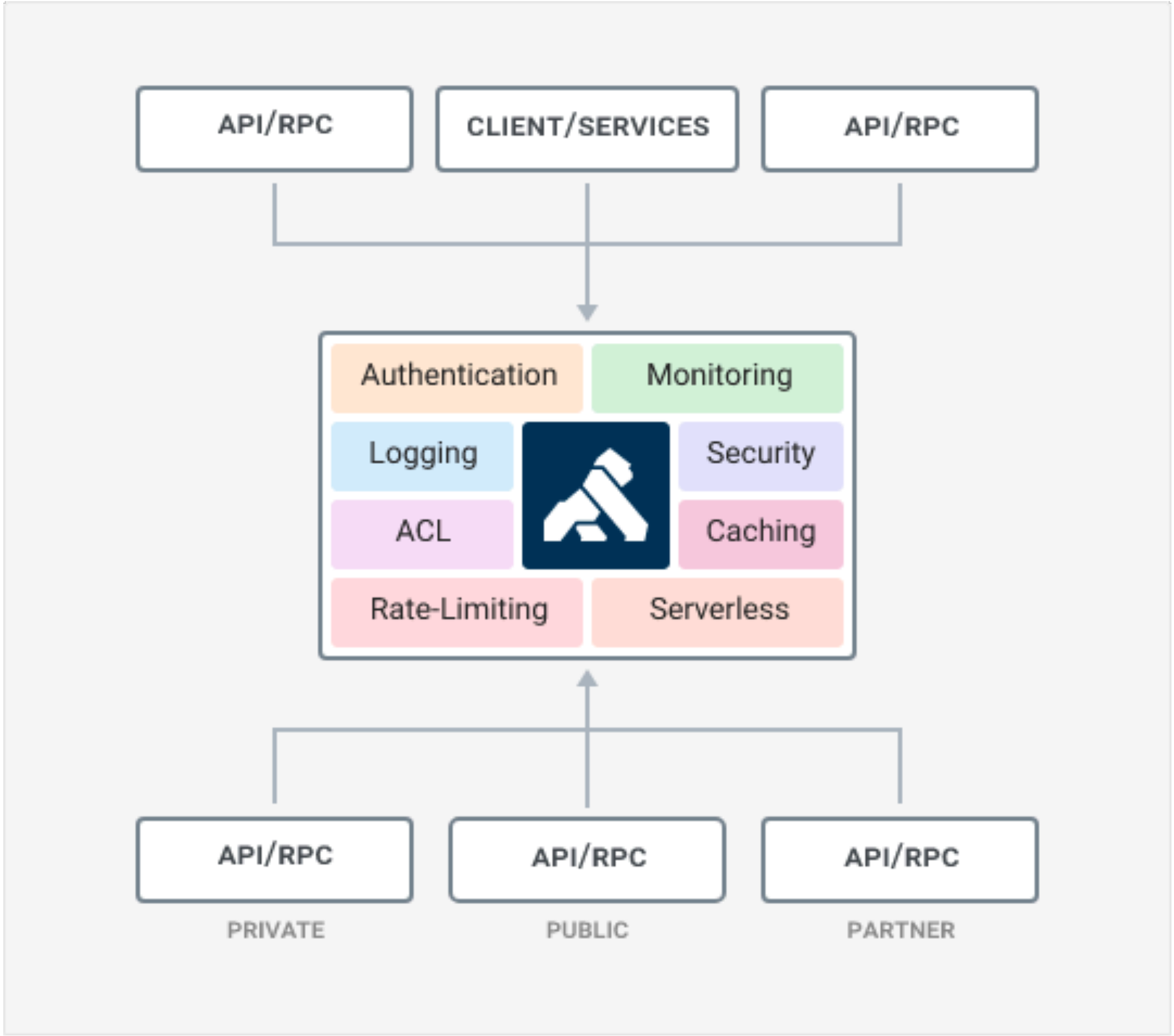
KONG-OPERATOR

https://github.com/upmc-enterprises/kong-operator

KONG API GATEWAY

- Open source API Gateway
- Isolate traffic into our applications
- Handles Authentication (HMAC) for clients


CLIENT/SERVICES
API/RPC
Authentication
Rate-Limiting
PRIVATE
API/RPC
Authentication
Rate-Limiting
Logging
Caching
Serverless
PUBLIC
API/RPC
Authentication
Rate-Limiting
Monitoring
PARTNER

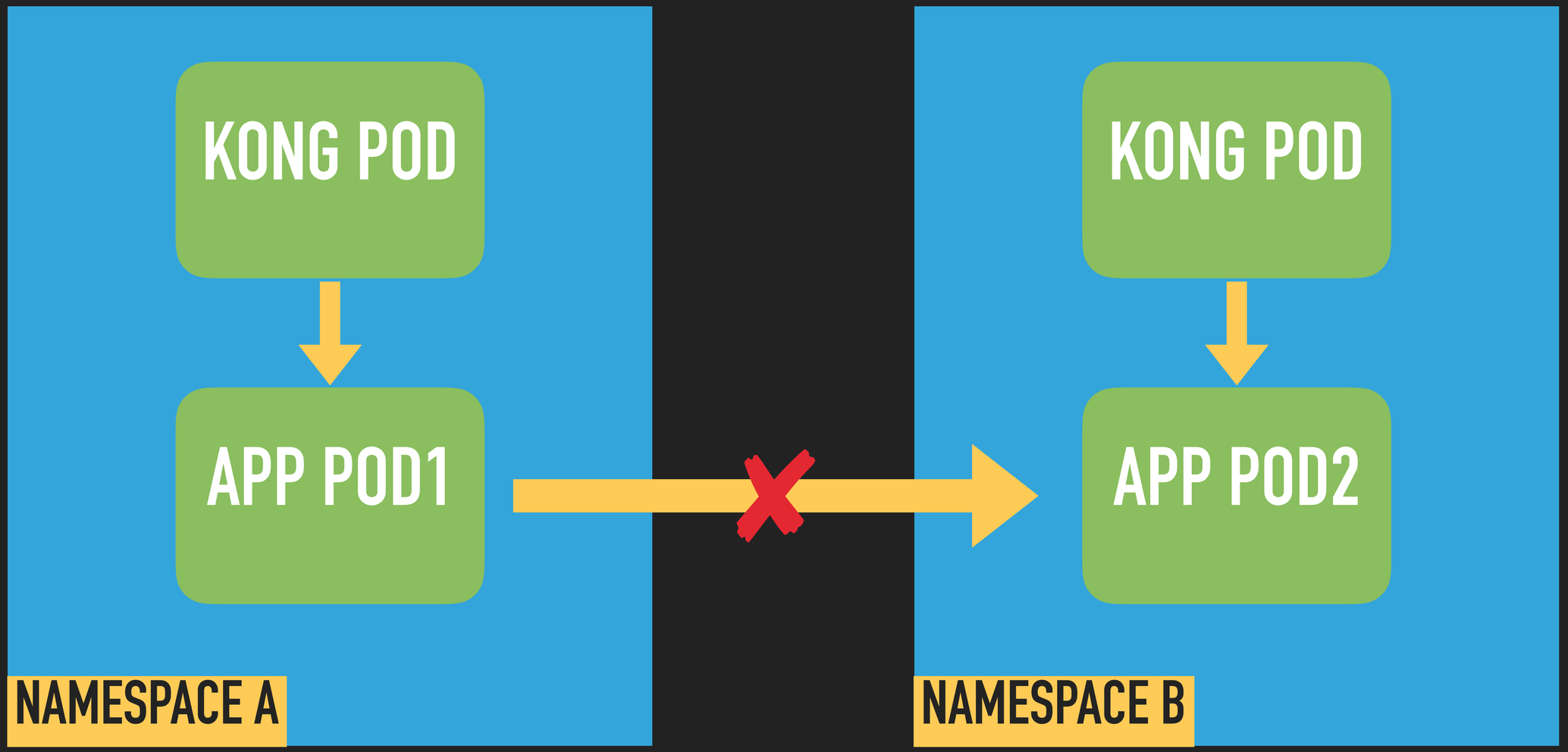

API/RPC
CLIENT/SERVICES
API/RPC
Authentication
Monitoring
Logging
Security
ACL
Caching
Rate-Limiting
Serverless
API/RPC
API/RPC
API/RPC
PRIVATE
PUBLIC
PARTNER

KONG OPERATOR

- Configuration for applications stored as files (TPRs)
  - Checked into source
  - Code reviewed
  - HTTP is not easily reproducible

NETWORK POLICIES

- Limit access to API



Steve Sloka

Senior Systems Software Engineer - Customer Success

Heptio empowers the technology driven enterprise to realize the full potential of Kubernetes. We offer training, support and professional services to speed integration of Kubernetes and related technologies into the fabric of your IT.

github.com/stevesloka

@stevesloka

http://stevesloka.com