AWS re:Invent

NOV. 29 – DEC. 3, 2021 | LAS VEGAS, NV

ARC326

Beyond five 9s: Lessons from our highest available data planes

Colm MacCárthaigh
VP/Distinguished Engineer
AWS

Yasemin Avcular
Principal Engineer
AWS

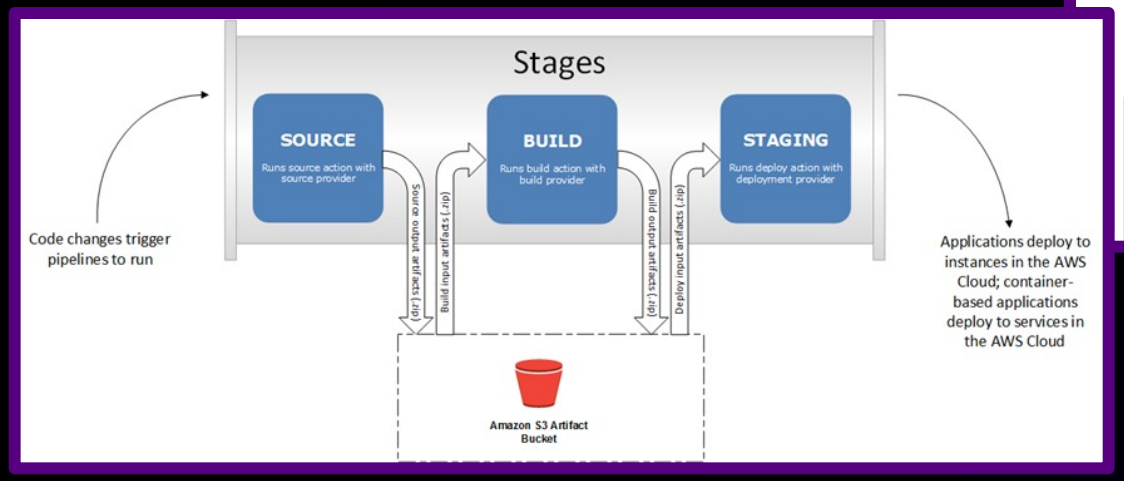
1: Insist on the highest standards

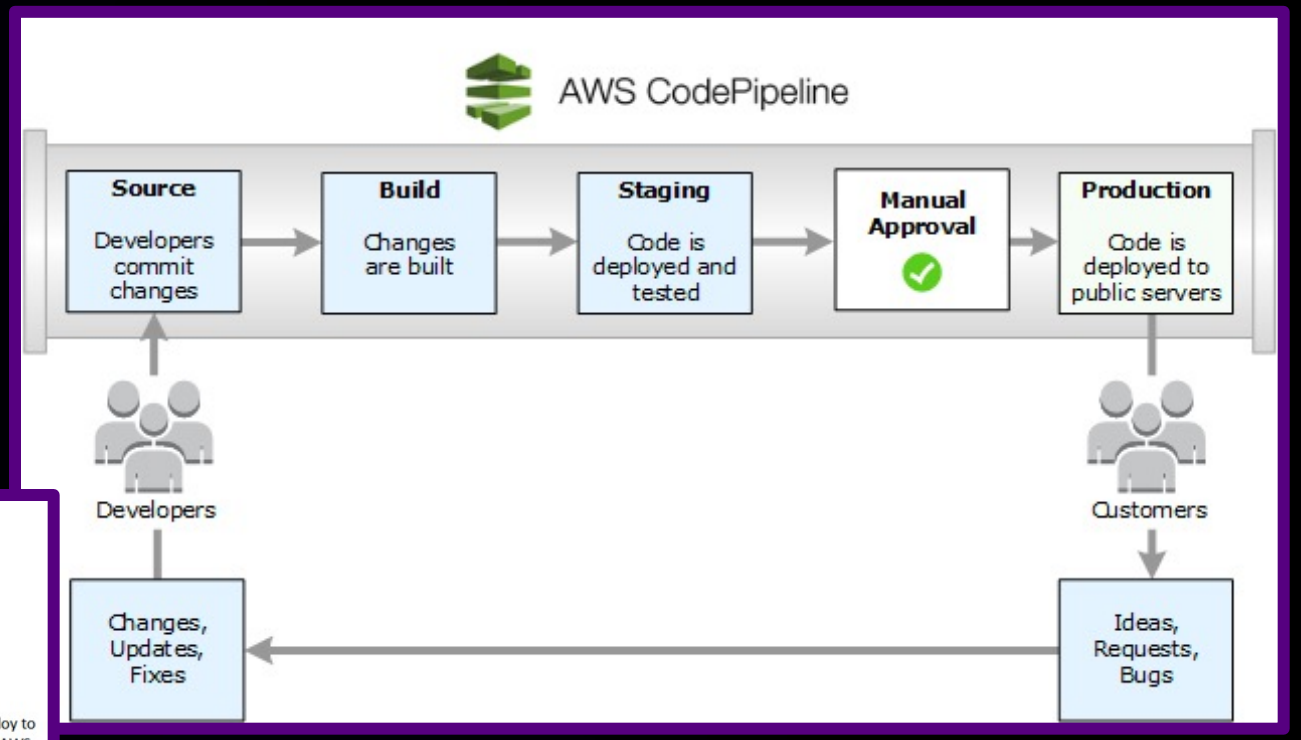
Insist on the highest standards

"Culture eats strategy for breakfast"
Peter Drucker

"Quality is a habit, not an act"
Aristotle

Deployment Safety





Deployment Safety

New code means risk, so we are incredibly paranoid about deploying it

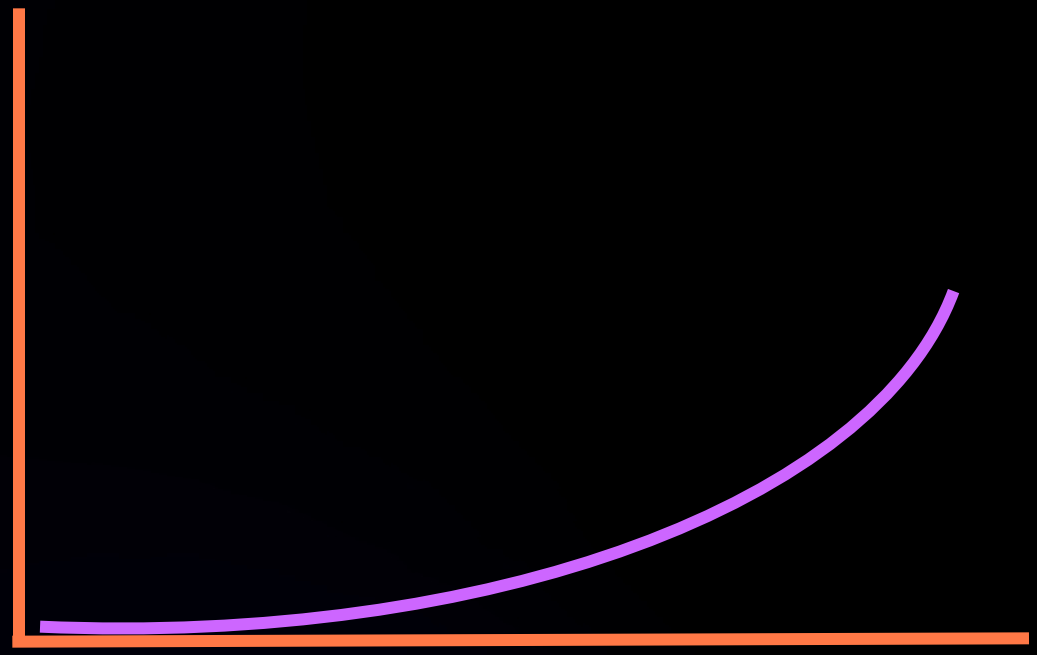
CI/CD staged deployment process

Promotion testing and monitoring at every stage, with automated rollback

Fast and reliable rollback

Deployment Safety

1. Code-review
2. Check-in
3. Pre-Production
4. One Box
5. One Availability Zone
6. One Region
7. Onwards …



2: Cattle vs. Pets

Cattle vs. Pets

Most systems at AWS are beyond a scale that can be managed by hand

We use auto scaling groups, VPCs, subnets, security groups, and more as units of abstraction

Our deployment systems clone infrastructure between Regions

Cattle vs. Pets

AWS operators don’t have access to all AWS Regions

Services such as AWS Outposts, AWS Snowball, and AWS Snowmobile are designed to be disconnected for periods of time

Bastioned systems: limited access for recovery via “bastions,” with record and notification processes

Cloistered systems: systems with no general purpose, interactive, or administrative access

Cattle vs. Pets

Reduces possibility of any untracked changes

Improves security

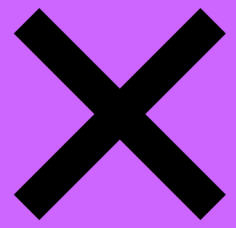
AWS Nitro System operators have no interactive access or general purpose access

3: Limit the Blast Radius

Regional Isolation

Regional Isolation

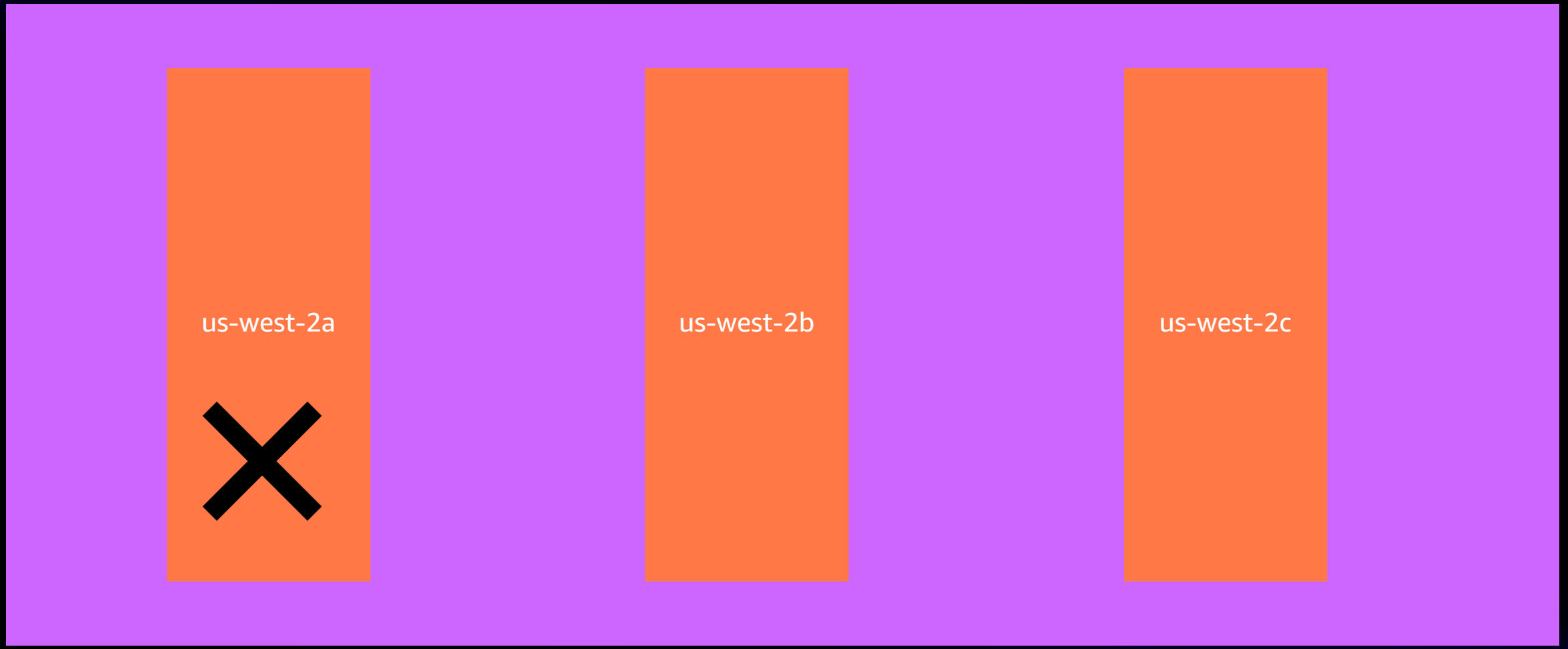
us-west-1



us-east-2

ap-east-2

Zonal Isolation



Cellular Isolation

Cellular Isolation

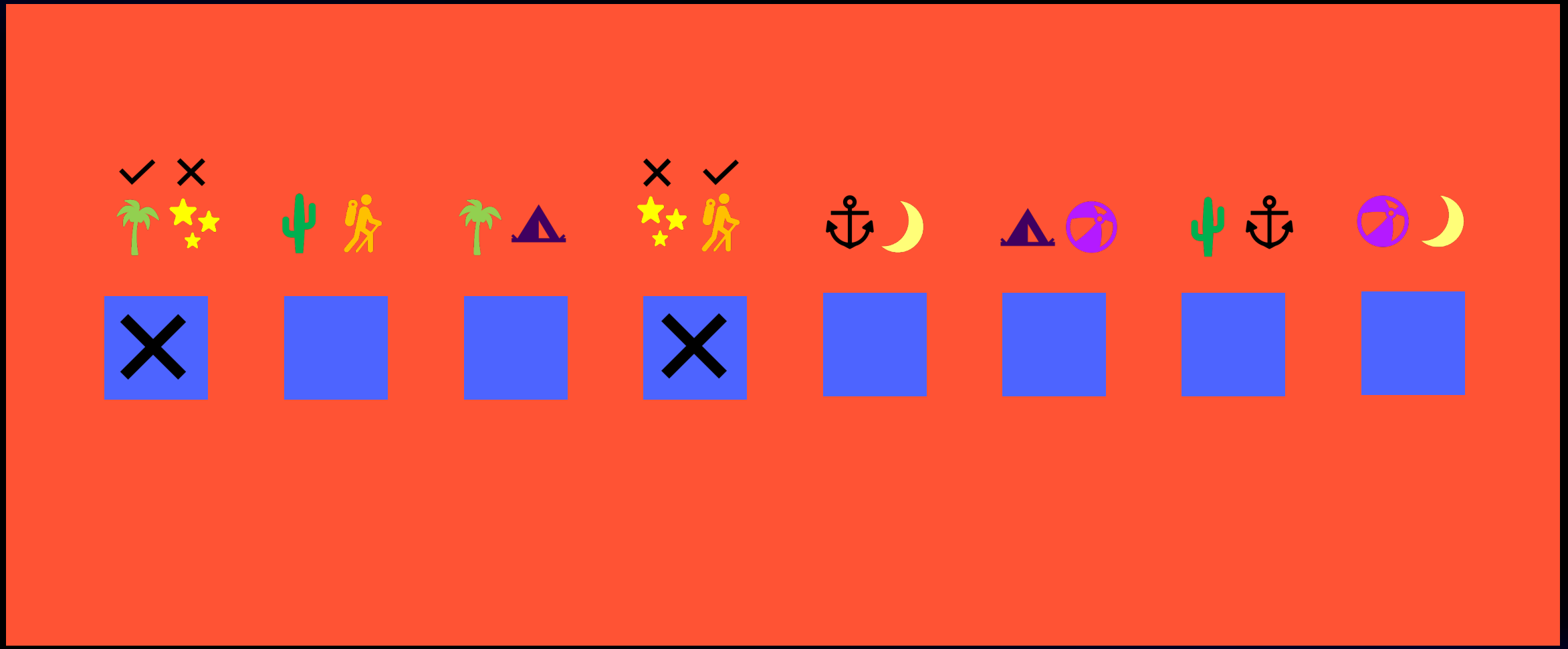
Cell 1

Cell 2

Cell 3

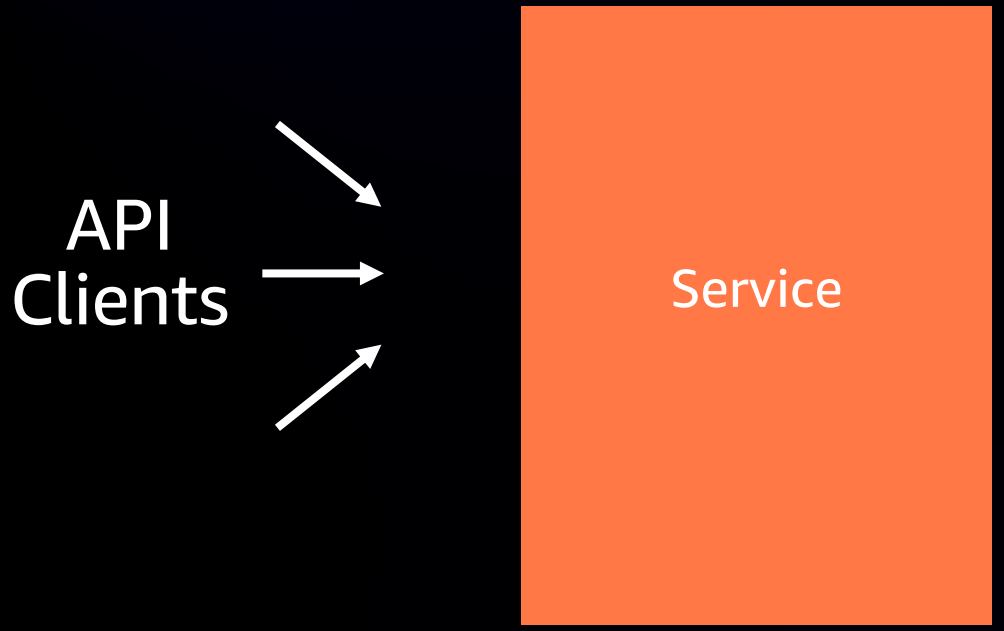
Cell 4

Shuffle Sharding

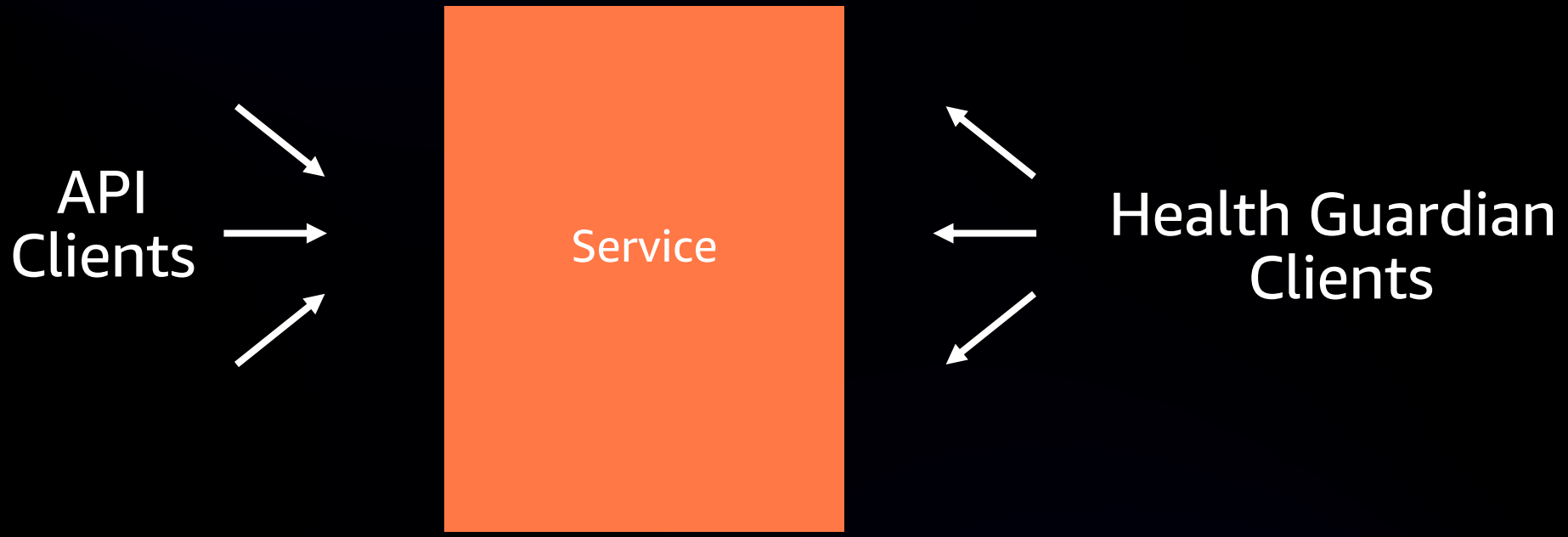


4: Circuit Breakers

Circuit Breaker – Load Shedding



Circuit Breaker – Bullet Counters



5: Raise the bar in Testing

Raise the bar for testing

1000s of Unit tests

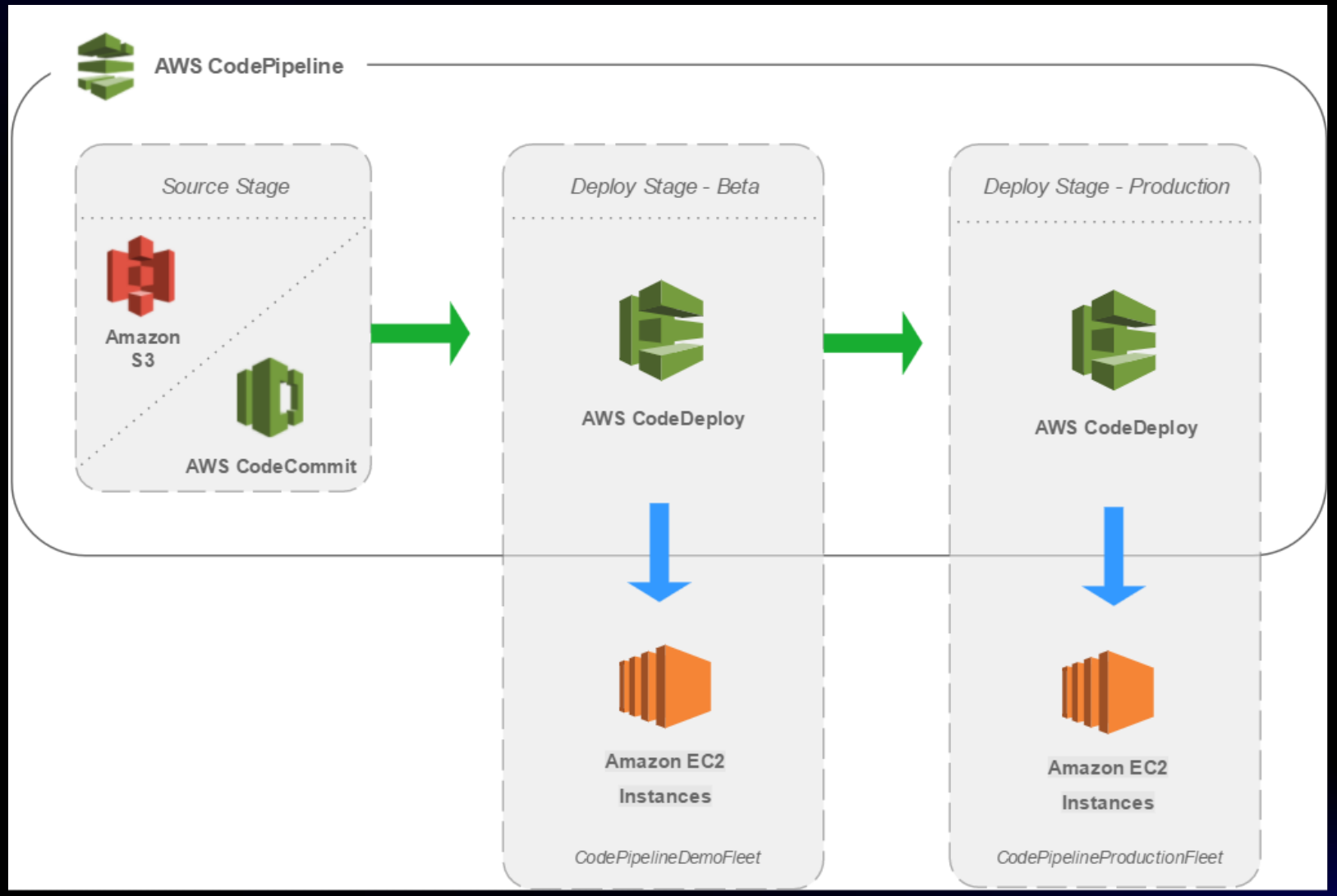
100s of Integration tests

Pre-prod environments

Roll forward and roll back testing

```
Running s2n_hash_test.c                                    ... PASSED       161 tests
Running s2n_rc4_test.c                                     ... PASSED     28742 tests
Running s2n_map_test.c                                     ... PASSED     57418 tests
Running s2n_override_openssl_random_test.c                 ... PASSED        13 tests
Running s2n_handshake_test.c                               ... PASSED       232 tests
Running s2n_ecc_test.c                                     ... PASSED        30 tests
Running s2n_stuffer_test.c                                 ... PASSED       701 tests
Running s2n_3des_test.c                                    ... PASSED     27248 tests
Running s2n_stuffer_hex_test.c                             ... PASSED       319 tests
Running s2n_pem_rsa_dhe_test.c                             ... PASSED        50 tests
Running s2n_aes_test.c                                     ... PASSED     54189 tests
Running s2n_fragmentation_coalescing_test.c                ... PASSED        64 tests
Running s2n_aes_sha_composite_test.c                       ... PASSED    196450 tests
Running s2n_malformed_handshake_test.c                     ... PASSED        82 tests
Running s2n_hmac_test.c                                    ... PASSED       392 tests
Running s2n_record_test.c                                  ... PASSED    179817 tests
Running s2n_client_extensions_test.c                       ... PASSED       225 tests
Running s2n_self_talk_test.c                               ... PASSED  43000462 tests
Running s2n_self_talk_alpn_test.c                          ... PASSED  64500710 tests
Running s2n_drbg_test.c                                    ... PASSED   1000155 tests
Running s2n_random_test.c                                  ... PASSED 204480831 tests
Running s2n_cbc_verify_test.c                              ... PASSED   8641805 tests
Running s2n_aead_aes_test.c                                ... PASSED  29115201 tests
```

Raise the bar for testing



Raise the bar for testing

With Automated Reasoning and Formal Verification, we're going much further

We can prove that code is correct for any possible set of inputs

Getting easier and easier

Check out CBMC

6: Lifecycle Management

Lifecycle management

Modern security and compliance demands that credentials are frequently rotated

Expired and mismatched credentials can be a source of outages

It’s important to decouple expiry and alarming, and to explicitly manage the lifecycle of every credential

Lifecycle management

At AWS, we have “time to expiry” metrics for anything that expires

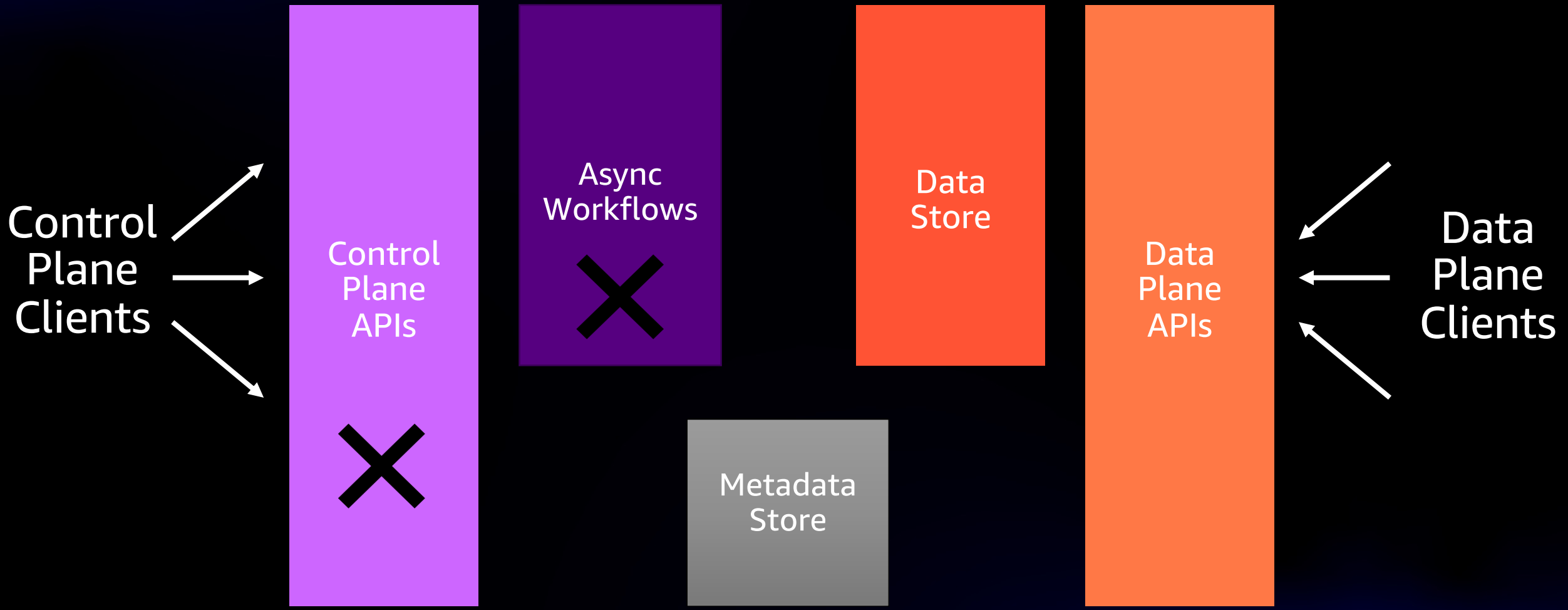
These metrics are both server-side and client-side

Alarm and investigate well before any problem

Additional protection from fail-safe canaries scanning

7: Modular Separation

Modular Separation



8: Static Stability

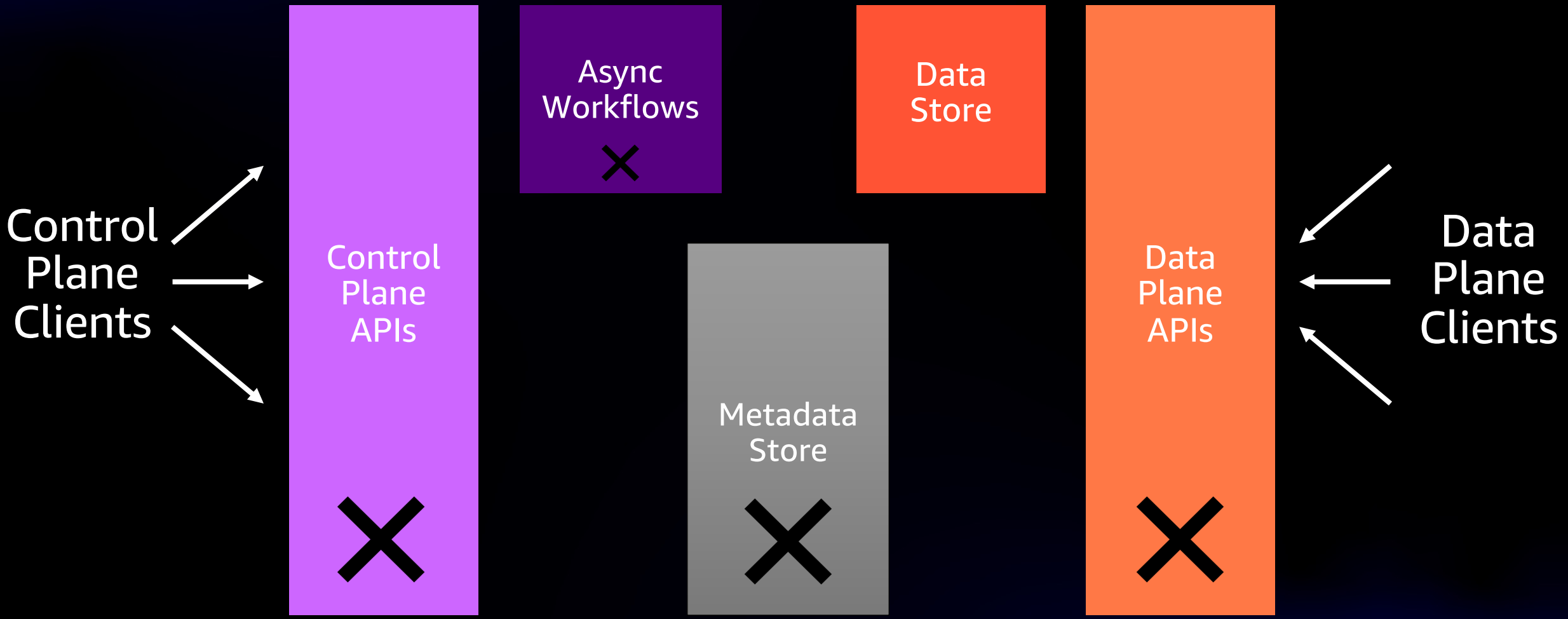
Static Stability

The availability of a system relies on availability of its dependencies

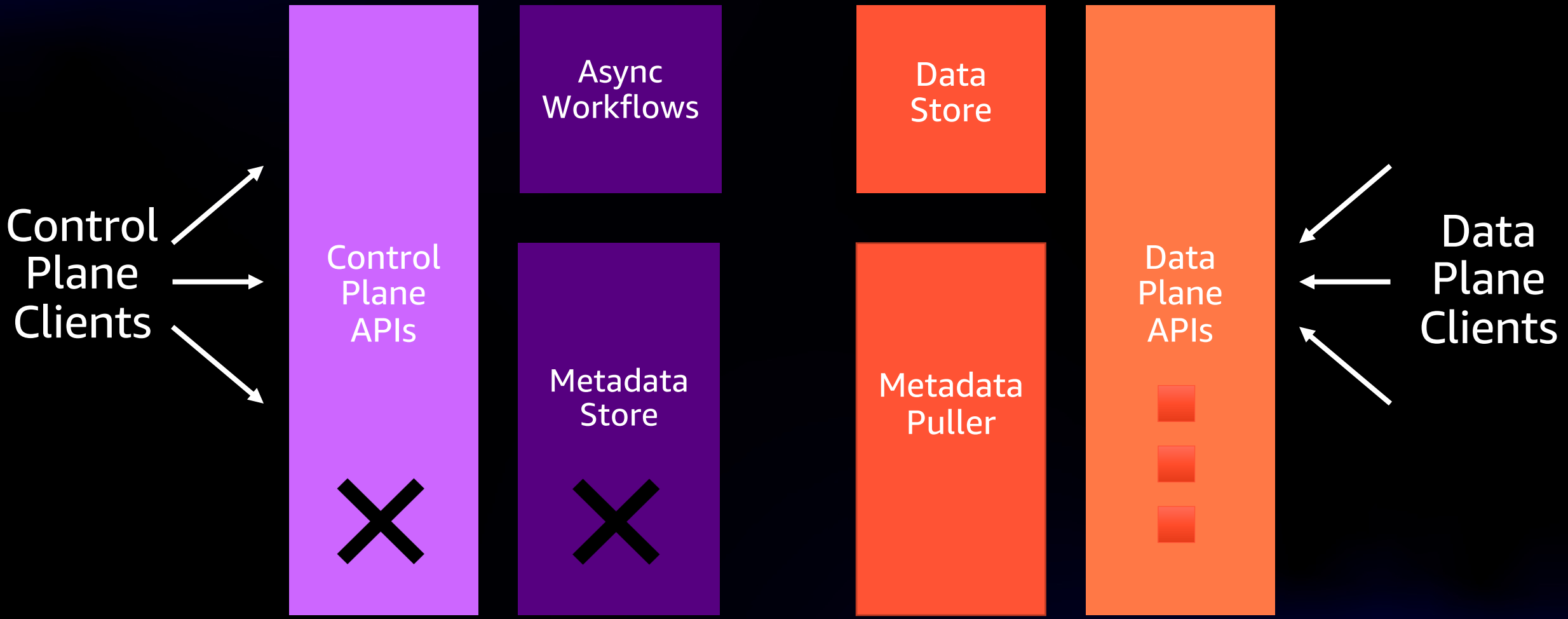
Systems should restore themselves into a safe working state with as few external dependencies as possible

“Turn it off and turn it on again” needs to work

Static Stability



Static Stability



9: Constant Work

Constant Work

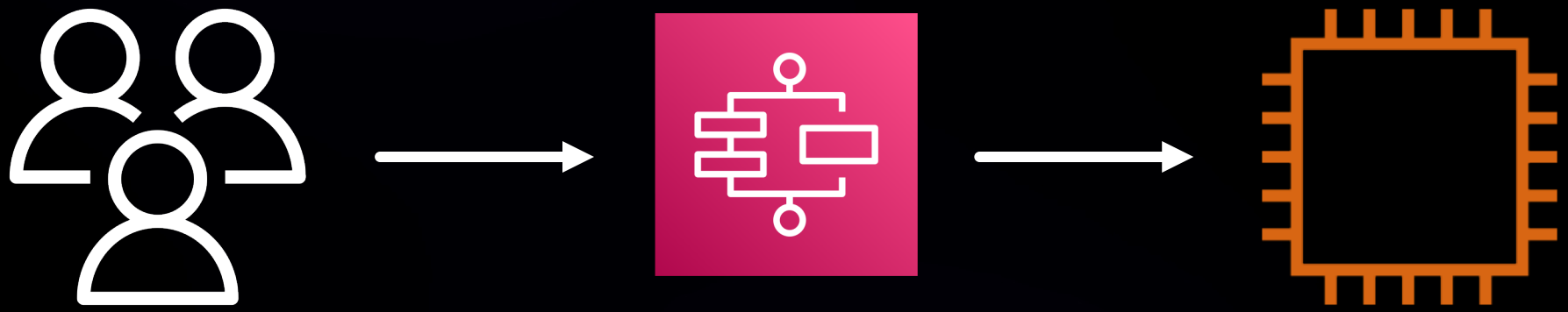
Risk is often proportionate to rates of change in systems

Example: a spike in load can slow down a system, which can cause knock-on and cascading effects

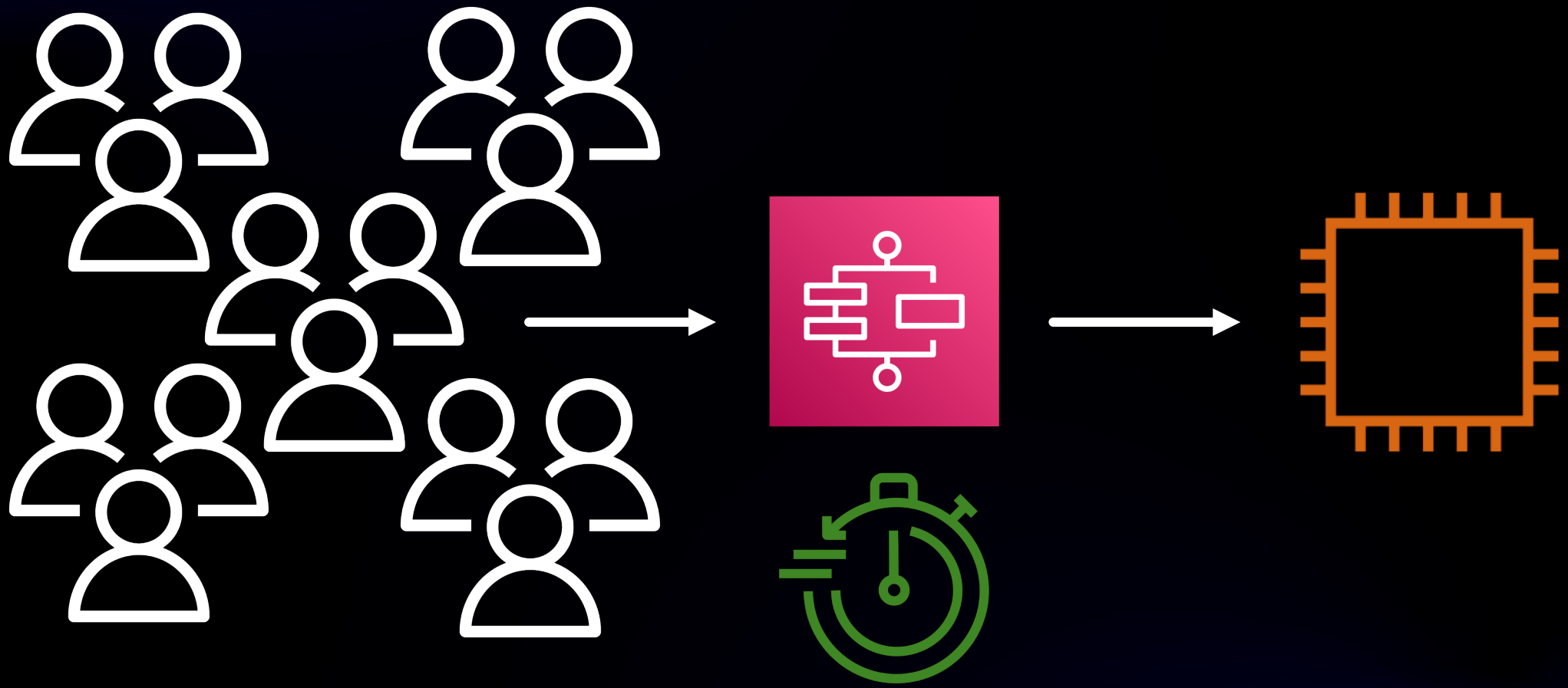
Reducing dynamism in systems is a great way to make them simpler

A counter-intuitive solution is to run the system at “maximum” load all the time, every time

Constant Work

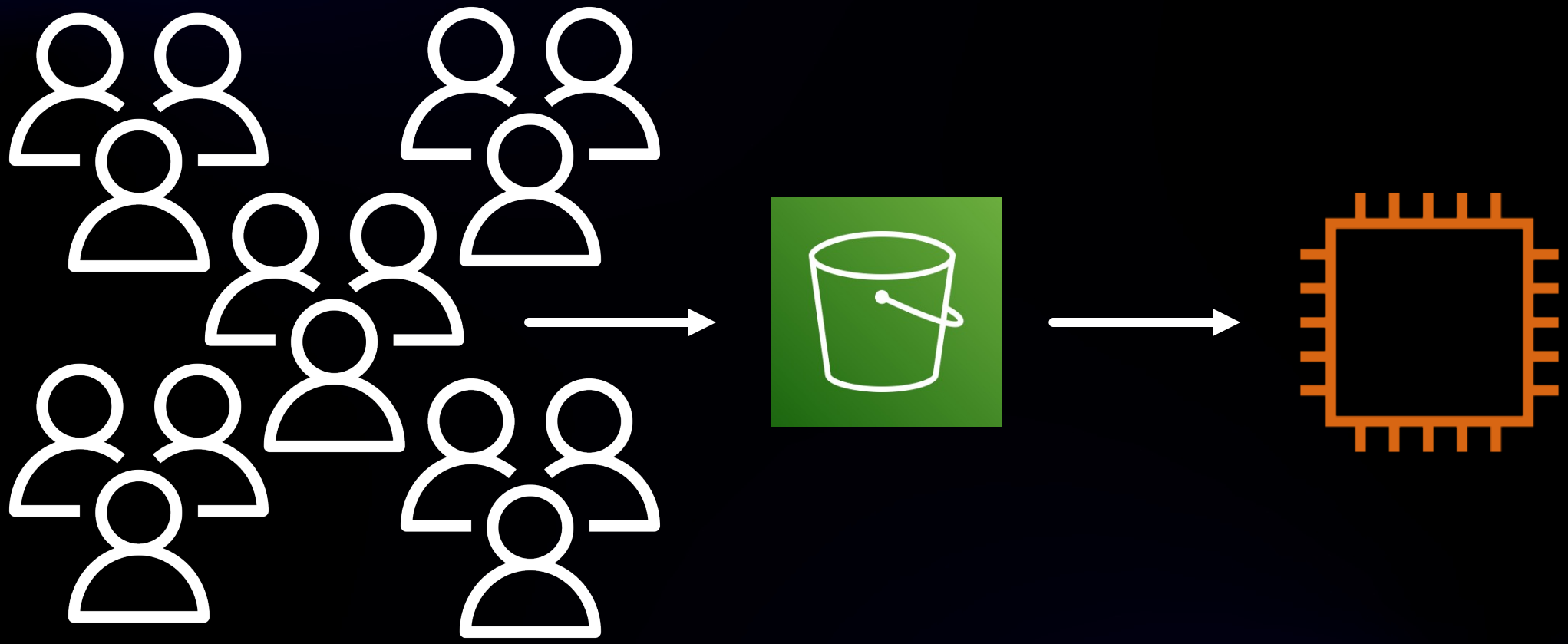


Constant Work



Constant Work

Constant Work



10: Retries

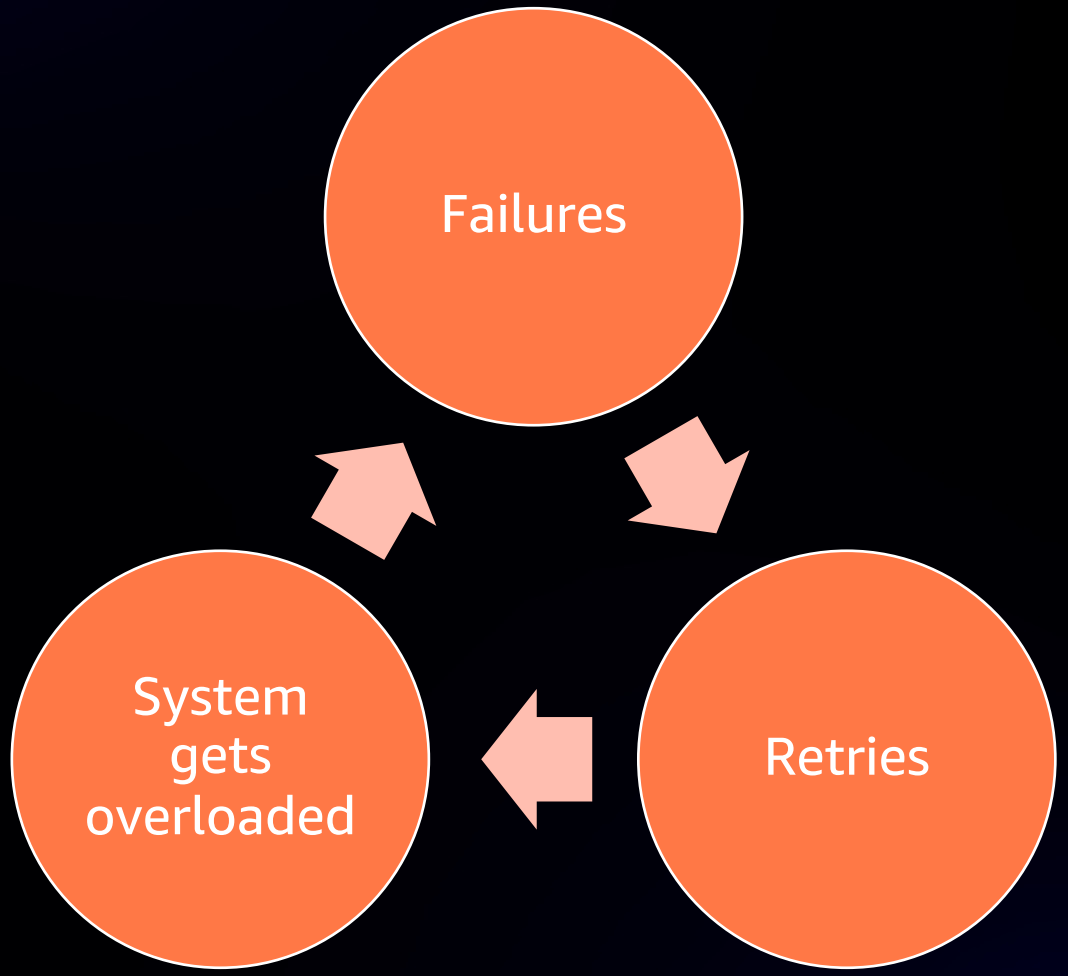
Retries

Thundering Herd

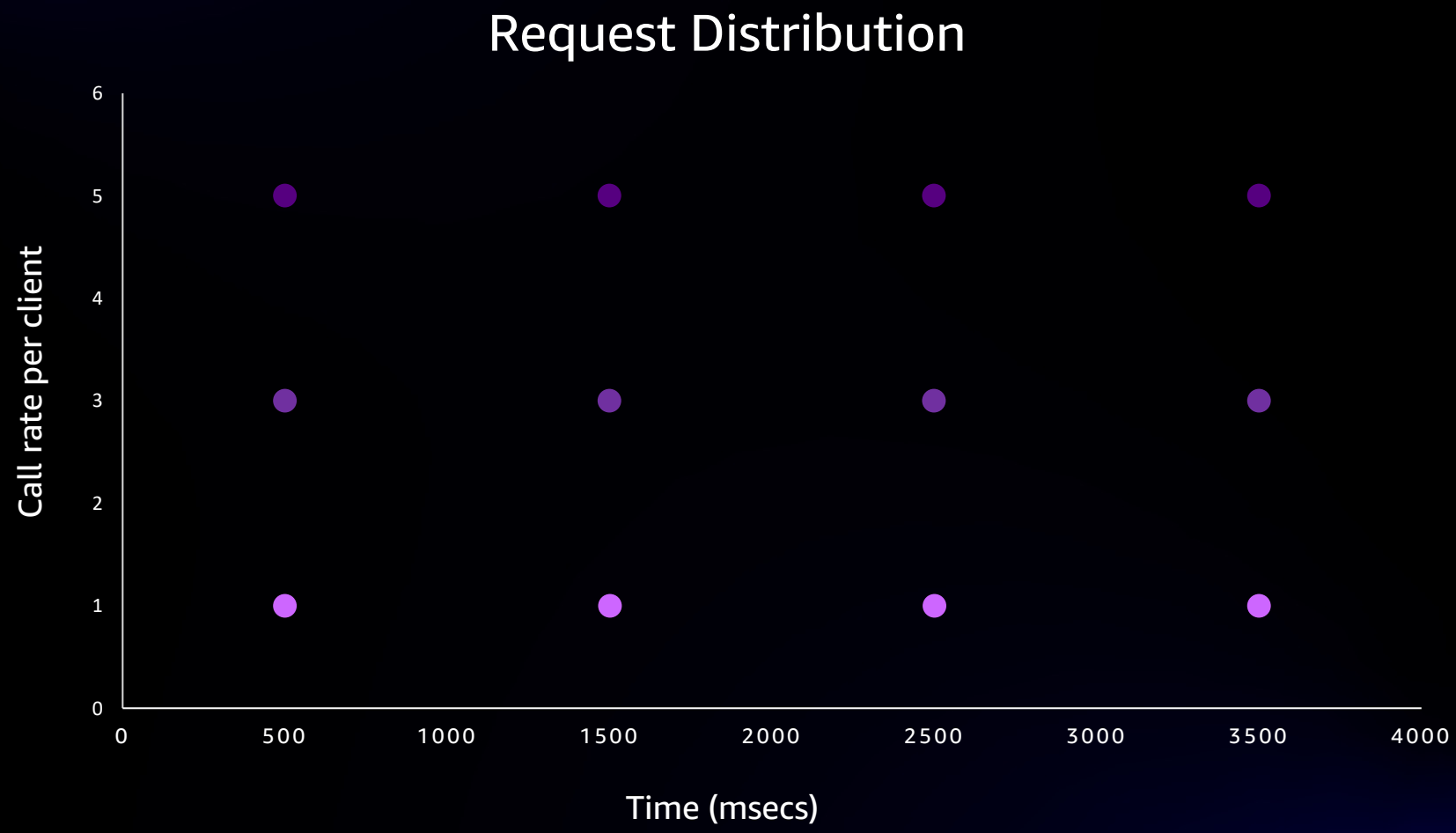
Exponential Backoff with Jitter

Client Throttling

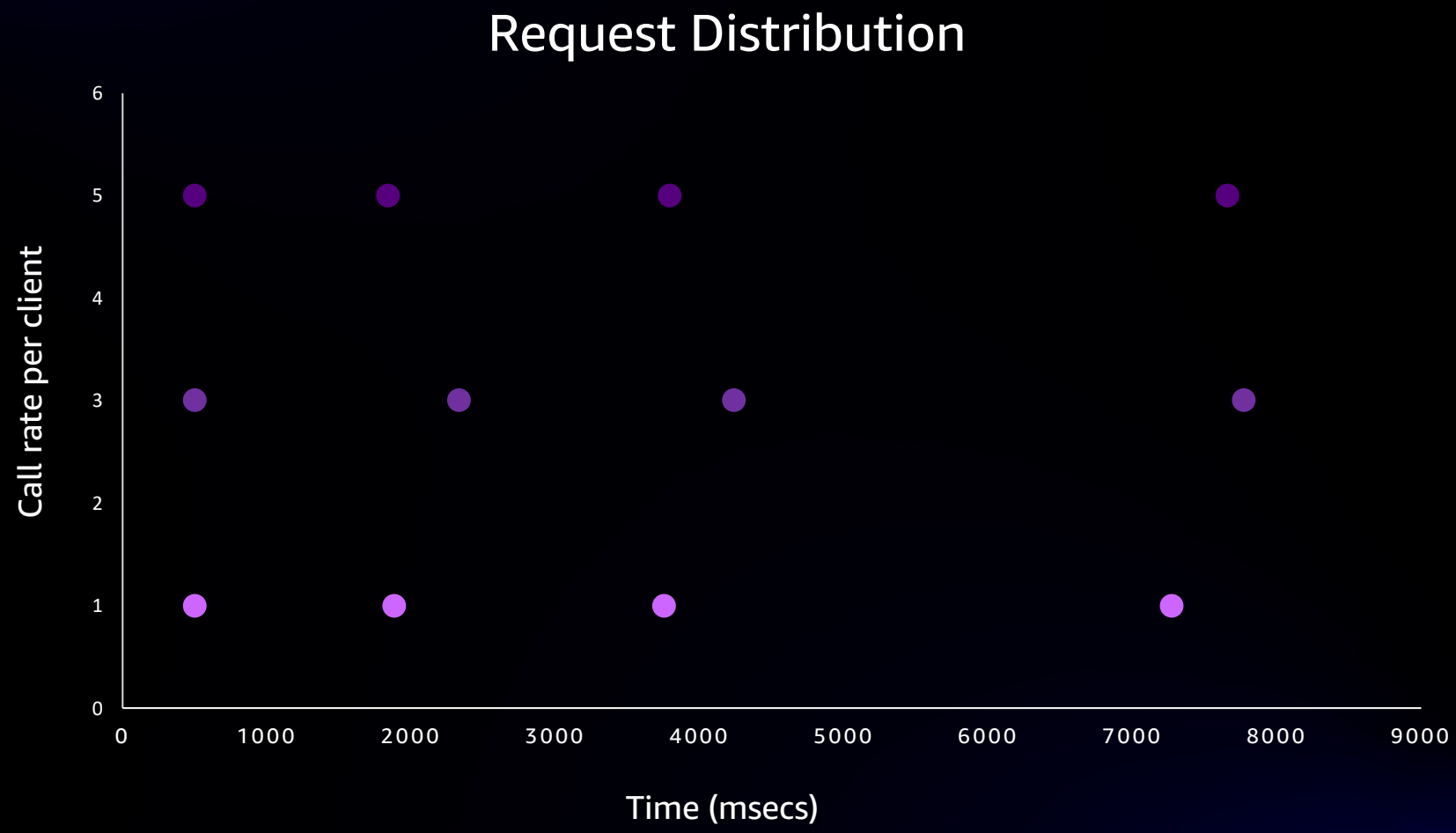
Retries – Thundering Herd



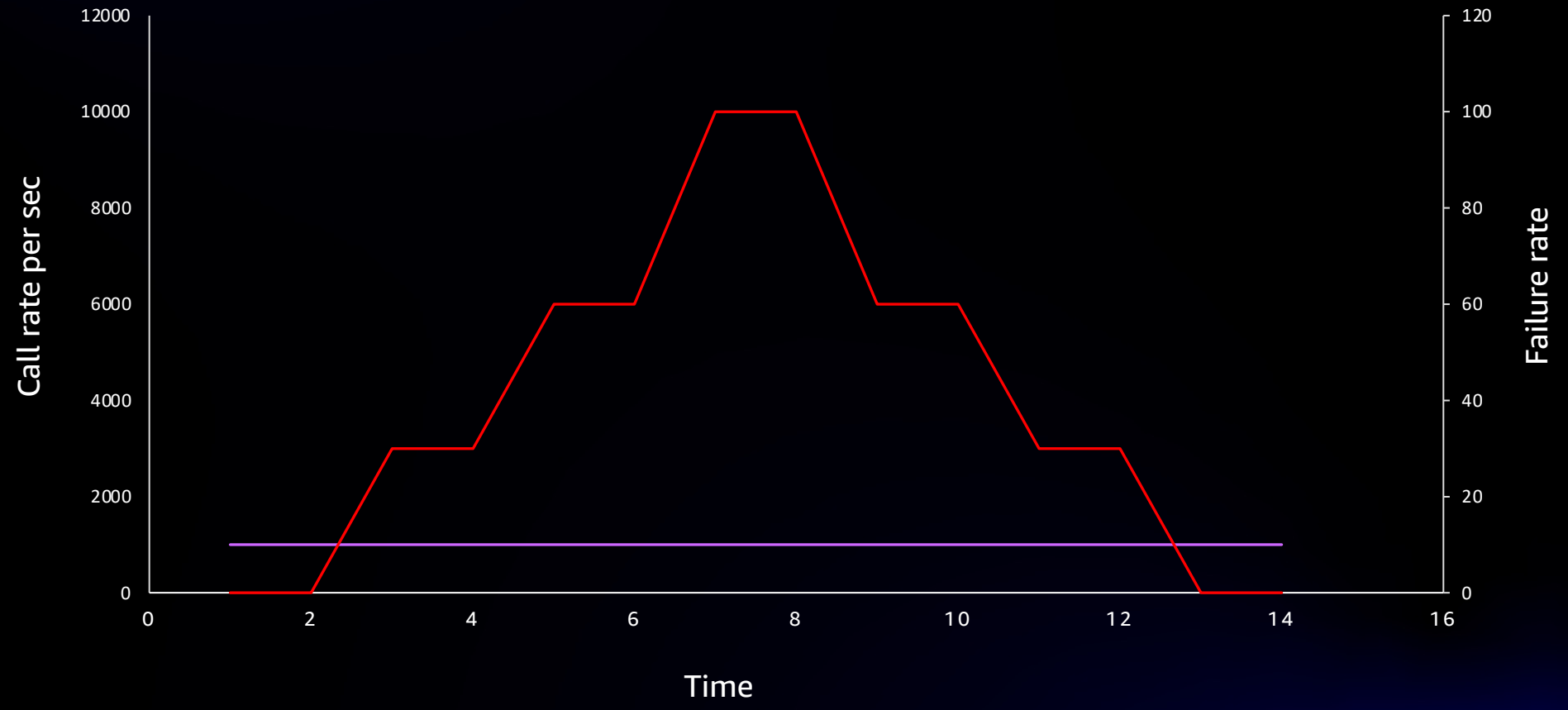
Retries – Exponential Backoff and Jitter



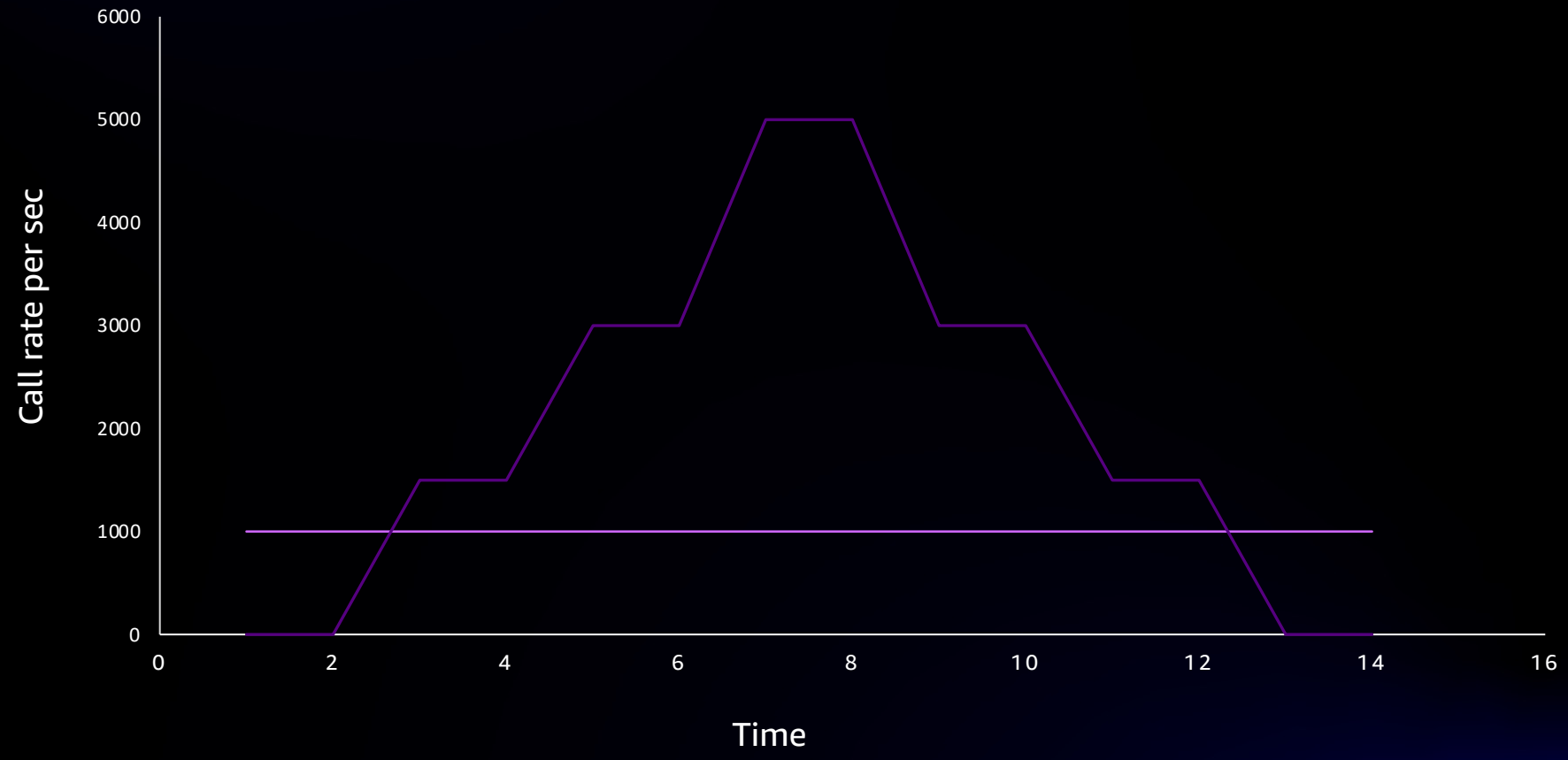
Retries – Exponential Backoff and Jitter



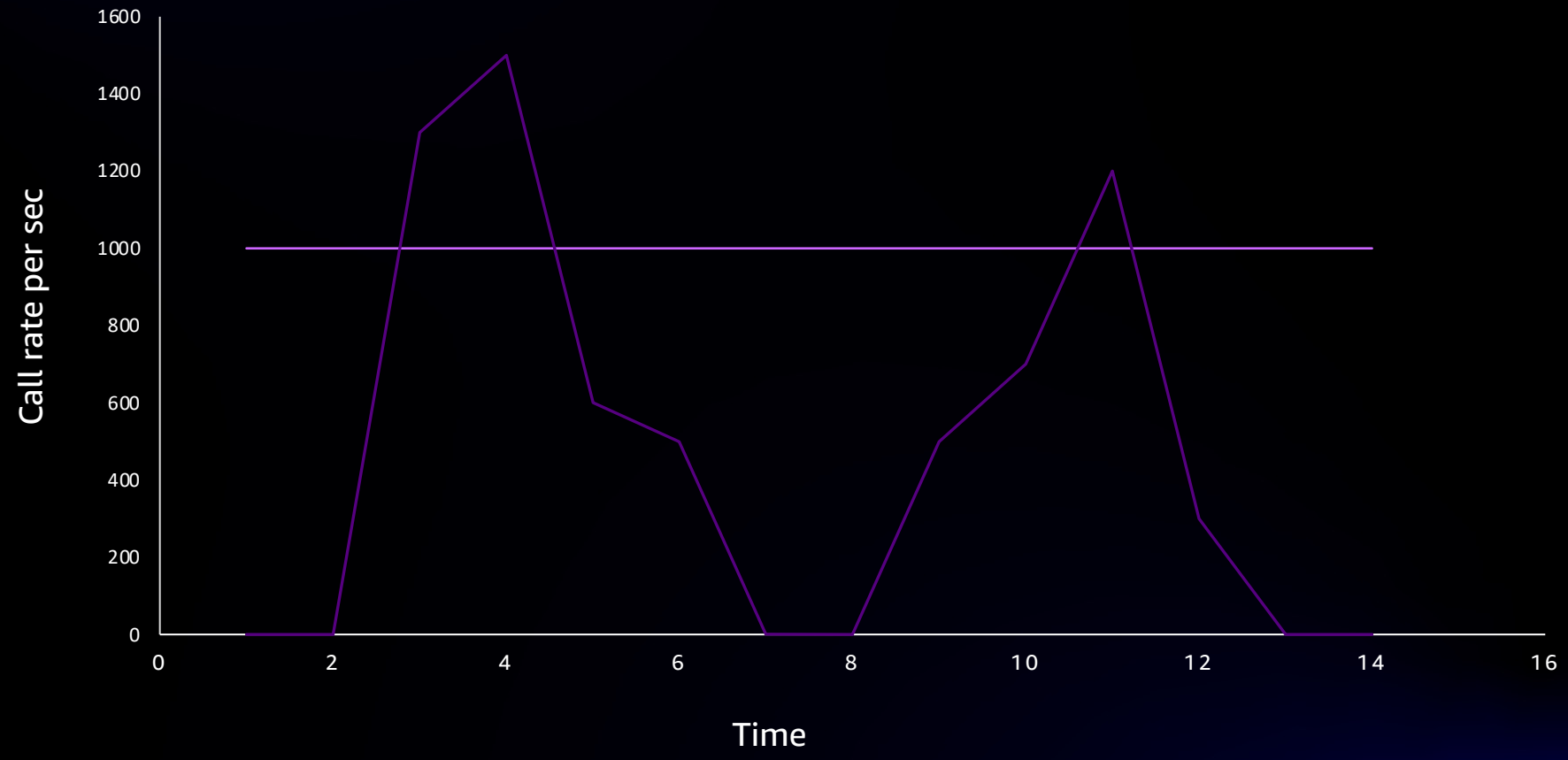
Retries – Client Throttling



Retries – Client Throttling



Retries – Client Throttling



Thank you!

Colm MacCárthaigh
colmmacc@amazon.com

Yasemin Avcular
yasemin@amazon.com