



# EOSDIS

NASA'S EARTH OBSERVING SYSTEM  
DATA AND INFORMATION SYSTEM

# Cost Controls in the Cloud

Summer ESIP 2019

Nathan Clark

EED-2 Cloud Solution Architect

[nathan.clark@nasa.gov](mailto:nathan.clark@nasa.gov)

This work was supported by NASA/GSFC under Raytheon Co. contract number NNG15HZ39C.  
This document does not contain technology or Technical Data controlled under either the U.S. International Traffic  
in Arms Regulations or the U.S. Export Administration Regulations.

# Elements of a Well Architected Cloud Governance Solution



## End User Access

Methods of access to the cloud environment



## Security Services

Central log aggregation and security event analysis



## Common Services

Infrastructure and Shared services accessible by cloud tenants



## Certification and Accreditation Strategy

Methodology to reach ATO fast with a repeatable process



## Networking

Enterprise networking strategy for intra-AWS  
Account communication and ingress/egress control



## Governance of Cloud Accounts

Tools for account management, budget enforcement, compliance automation + Access to CSP CLI, API, Console

# Elements of a Well Architected Cloud Governance Solution



**End User Access**  
Methods of access to the cloud environment



**Security Services**  
Central log aggregation and security event analysis



**Common Services**  
Infrastructure and Shared services accessible by cloud tenants



**Certification and Accreditation Strategy**  
Methodology to reach ATO fast with a repeatable process



**Networking**  
Enterprise networking strategy for intra-AWS  
Account communication and ingress/egress control



**Governance of Cloud Accounts**  
Tools for account management, budget enforcement, compliance automation + Access to CSP CLI, API, Console

# Goal

- Pay-as-you-go vs. up-front
- Adding hardware no longer a project
- Stick to budget without giving up flexibility

# Cost Conscious Development

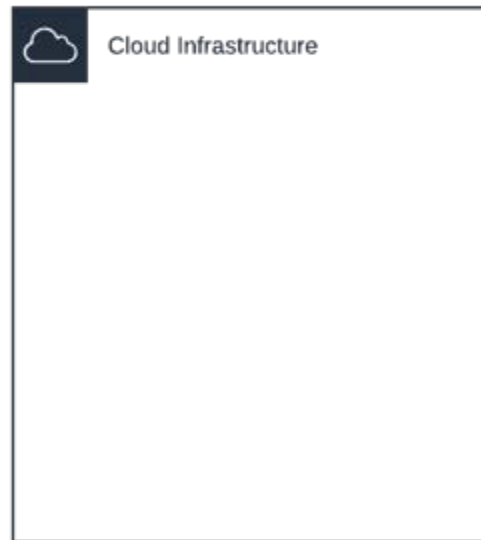
- Everything you do costs \$\$\$
  - Architecture choices impact system costs
  - Design choices impact system costs
  - Implementation choices impact system costs
- Cost Visibility
- Cost Controls

# Cost Control Patterns

# Cost Control

- Any monitoring, automated action or other tool that helps keep you from going over budget
- Internal vs. External
- Proactive vs. Reactive

# Internal vs. External

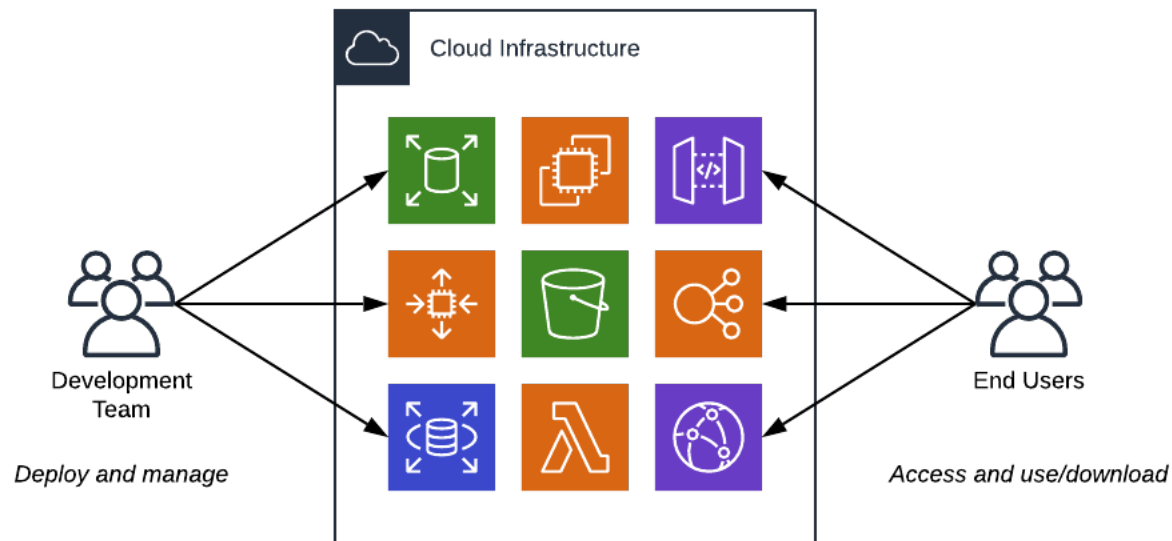




# Internal vs. External



# Internal vs. External



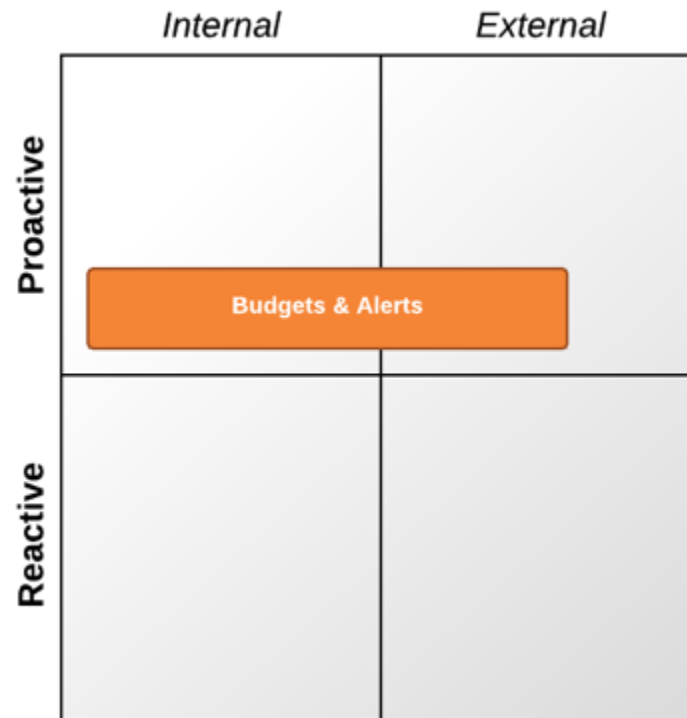
# Proactive vs. Reactive

- “Always on” vs. activated
- Proactive: Prevent or limit costs
- Reactive: React to costs
- [Cost] Defense in Depth

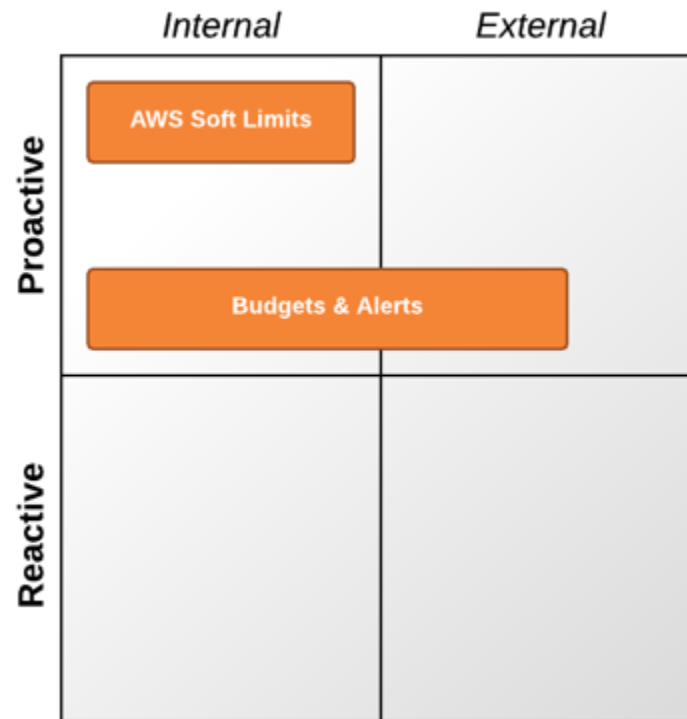
# Example Controls

	<i>Internal</i>	<i>External</i>
<b>Proactive</b>		
<b>Reactive</b>		

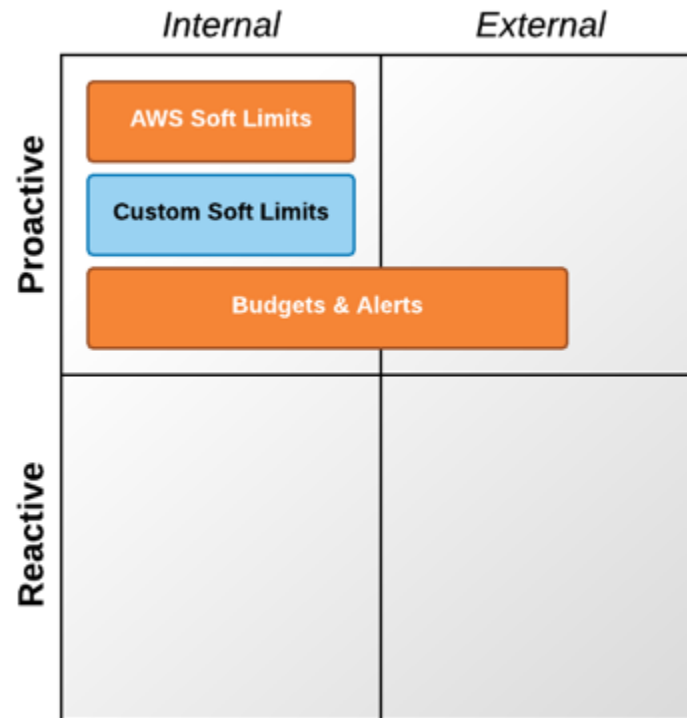
# Example Controls



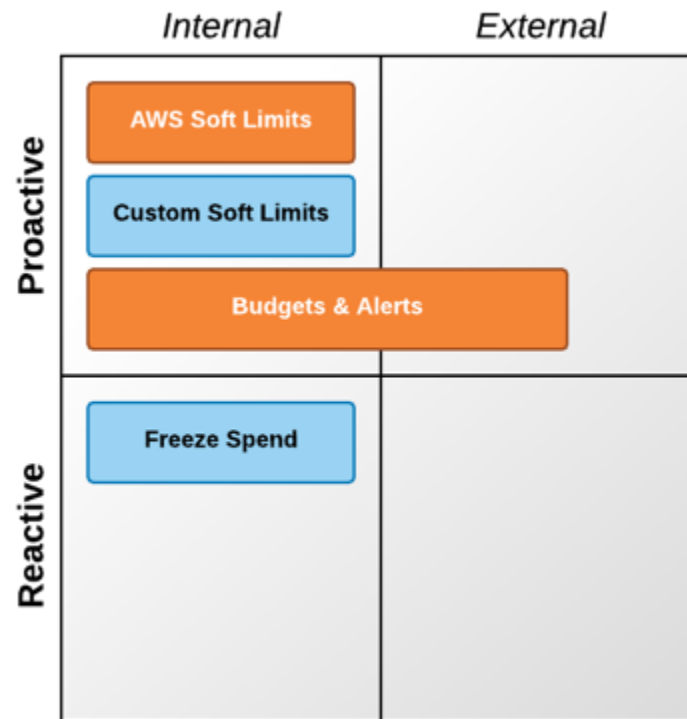
# Example Controls



# Example Controls

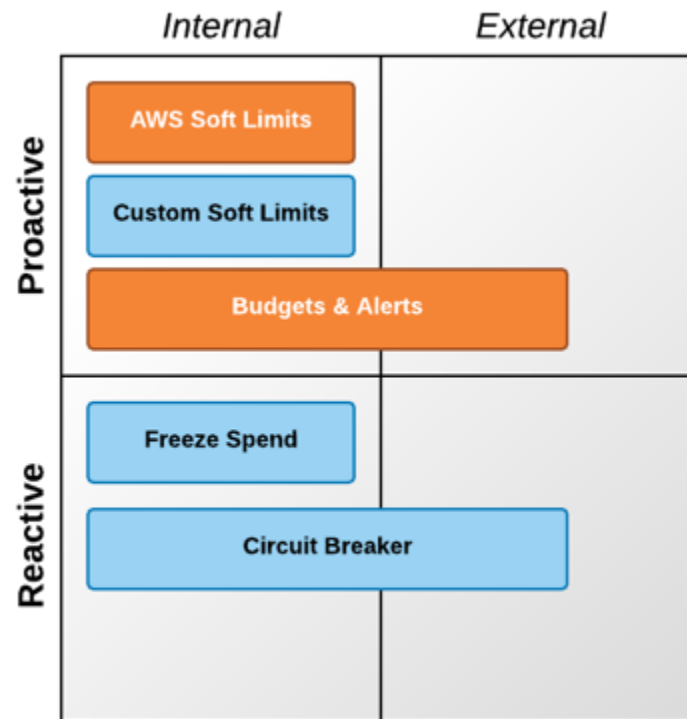


# Example Controls

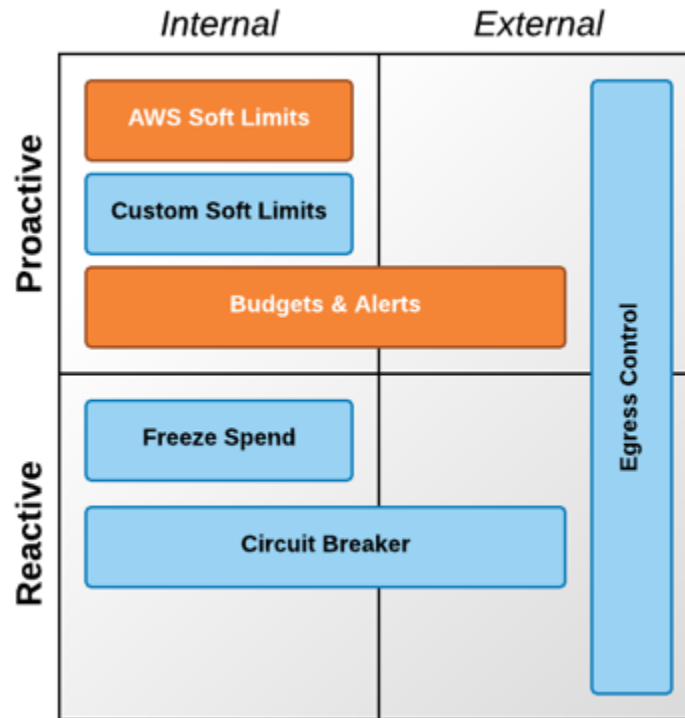




# Example Controls



# Example Controls



# Controlling Egress

# Why Egress Control?

- Not the biggest cost
- Harder to control
- Harder to predict

# Ways to Egress

- Egress = any data going out that costs you \$\$\$
- EC2/S3
  - Out to internet, or across regions
- CloudFront
  - Caching CDN
  - Cheaper than EC2/S3, even w/o caching
  - Price depends on edge node locations

# Ways to Egress

- Choose download mechanism based on user location
- Same region: unlimited, direct access
- Different region: limited, direct access
- Non-cloud: limited, through CloudFront

# Ways to Egress

- Custom application logic
- IAM policies
- Lambda@Edge
- AWS Published IP Ranges
  - <https://docs.aws.amazon.com/general/latest/gr/aws-ip-ranges.html>

# Throttling Egress

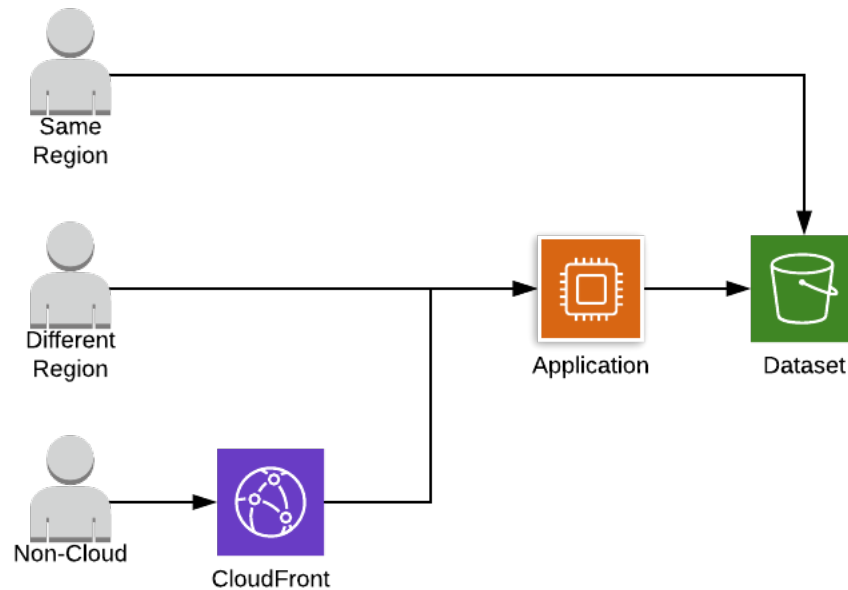
- Monitor request rates and bytes downloaded
- HTTP 429: Please Slow Down
  - Downside: users/scripts need to retry after a wait period
- Limit download bandwidth (proxy)



# Throttling Egress

- EC2 instance limits
- Network-layer throttling
- Application-layer throttling
- Custom vs. COTS

# Ways to Egress



**fin**

# Running Out

- Run out of money or run out of capacity
- Don't just plan for the happy path

# References

Cost Management in the AWS Cloud

<https://docs.aws.amazon.com/whitepapers/latest/cost-management/introduction.html>

<https://d1.awsstatic.com/whitepapers/aws-tco-2-cost-management.pdf> (PDF)

AWS Well-Architected Framework

<https://wa.aws.amazon.com/>

EC2Instances.info (instance type comparison)

<https://www.ec2instances.info/>

AWS IP Address Ranges

<https://docs.aws.amazon.com/general/latest/gr/aws-ip-ranges.html>

<https://ip-ranges.amazonaws.com/ip-ranges.json>

This work was supported by NASA/GSFC under Raytheon Co. contract number NNG15HZ39C.

# Raytheon

*in partnership with*

