Marginalise the Breach

A Zero-Trust Approach

Andrew Kay

Illumio Systems Engineer

illumio

Highest Value Assets

ACSC
AUSTRALIAN CYBER SECURITY CENTRE
NSW
GOVERNMENT
SWIFT
PCI DSS COMPLIANT
APRA
CPS 234

illumio

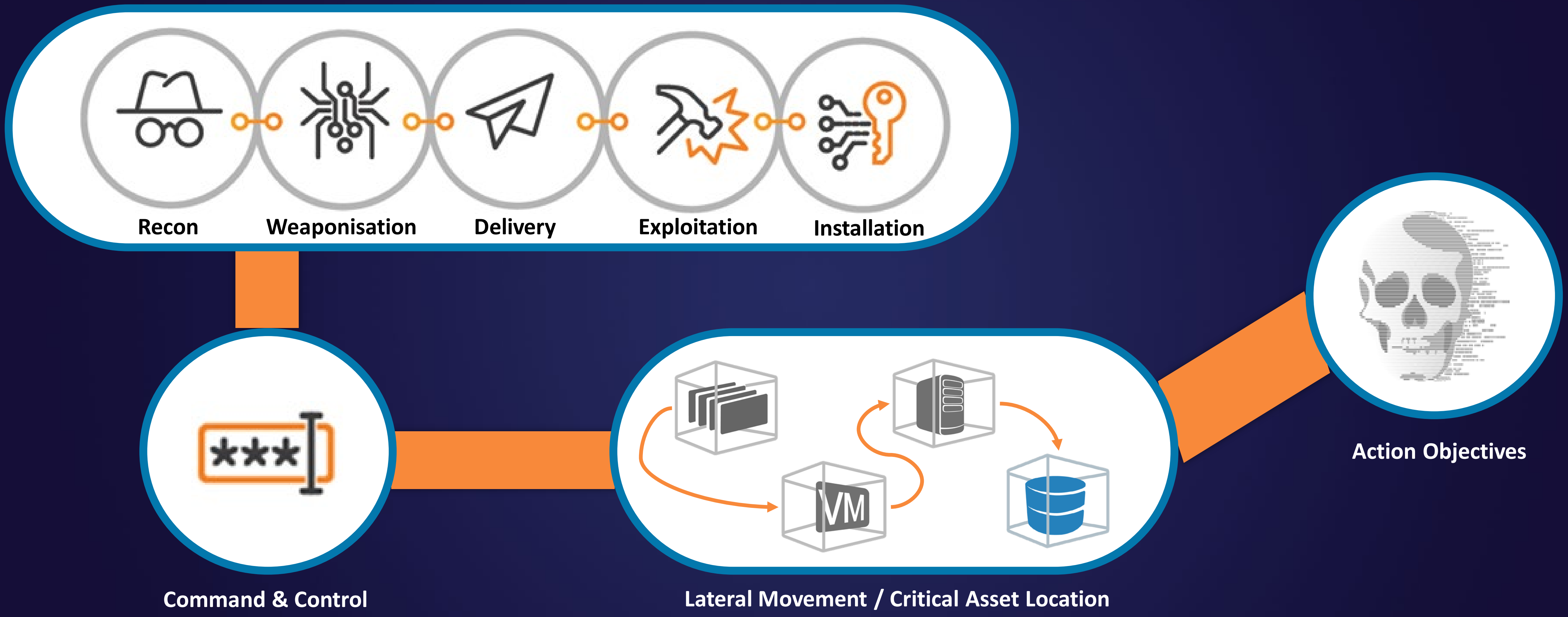
Exposures

☣ = **Exploitability** affects **Impact**

📍 = **Reachability** affects **Likelihood**

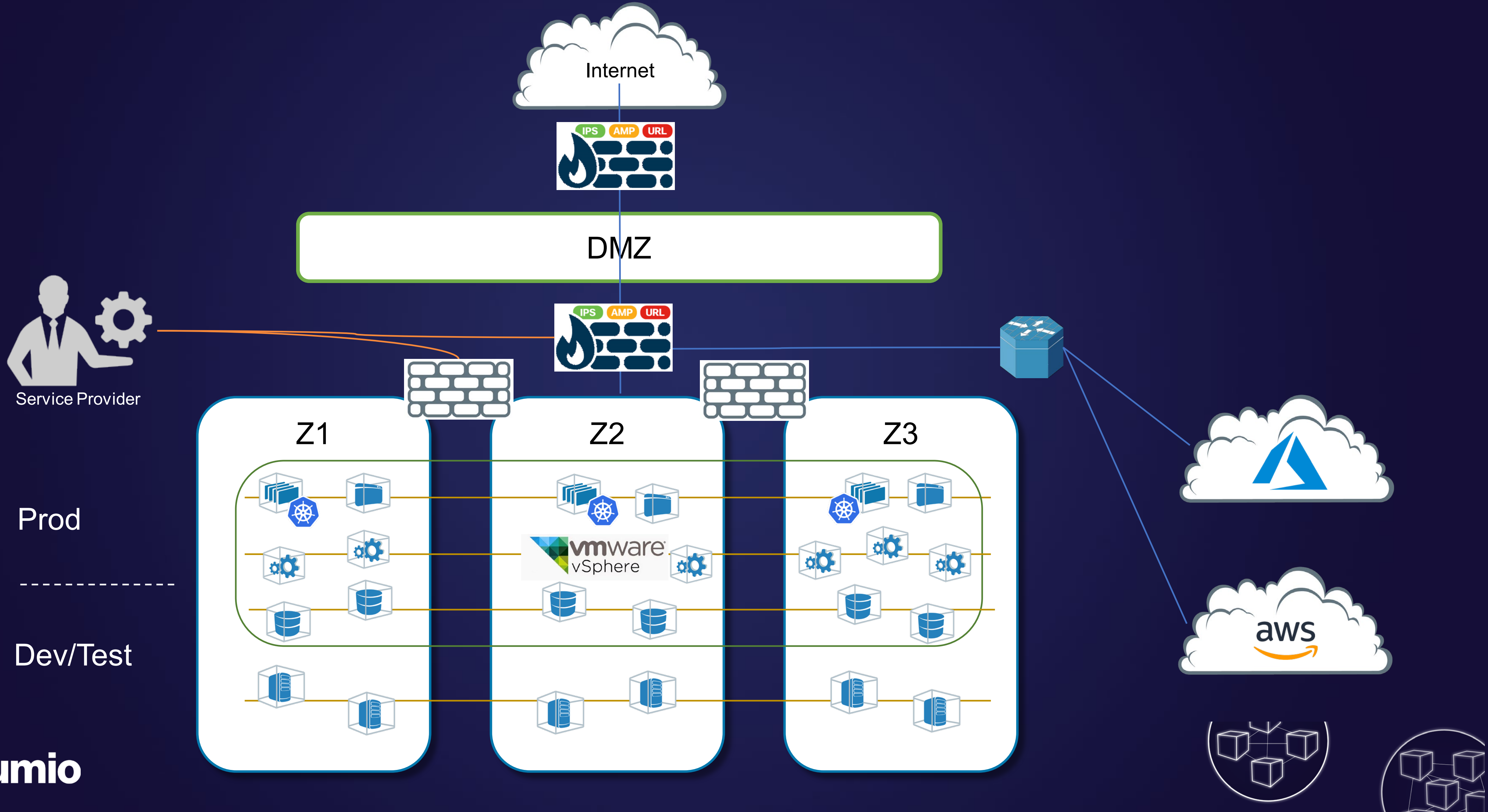
Likelihood is under our Control

Adversary Mobility



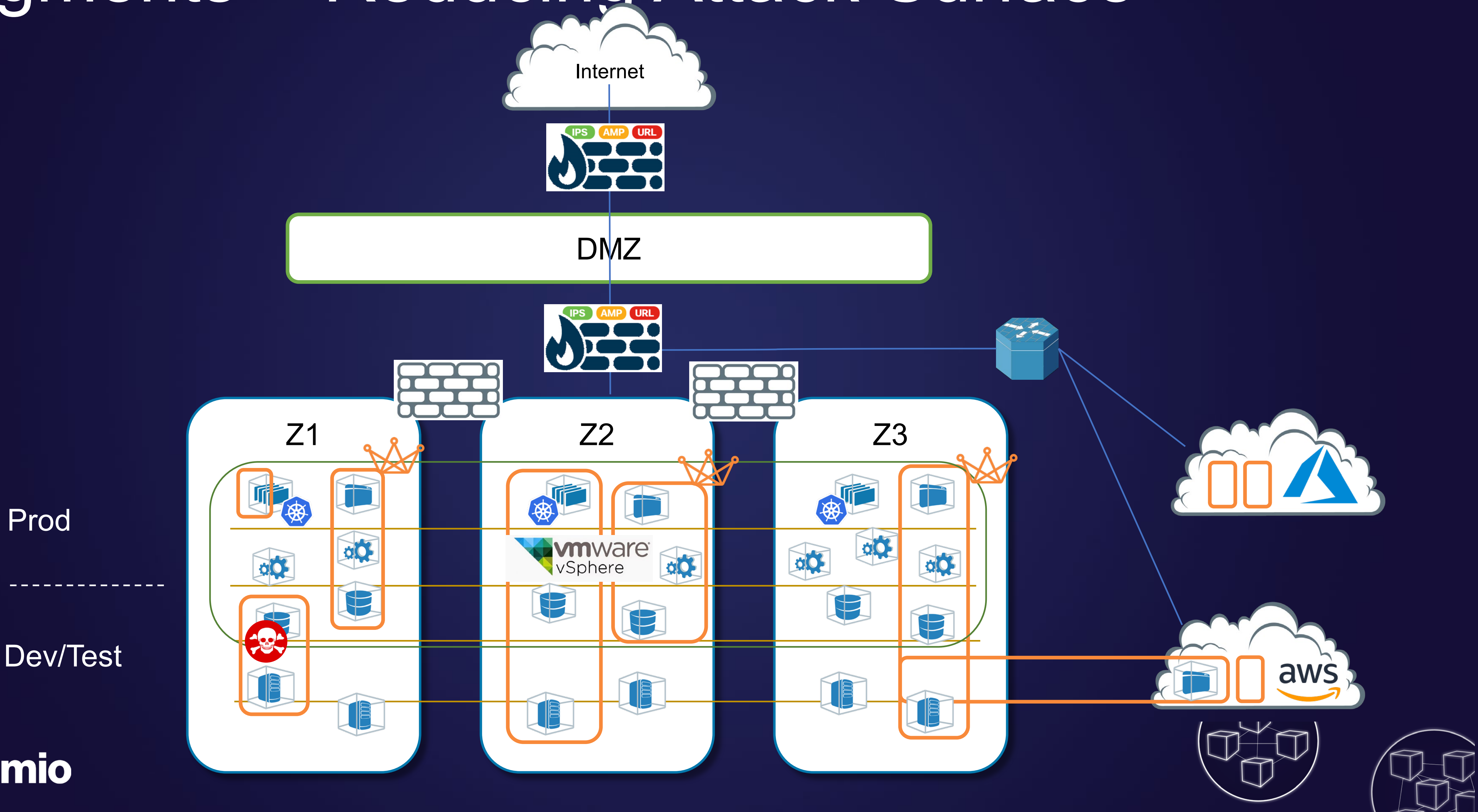
illumio

Traditional Model



illumio

Segments = Reducing Attack Surface



illumio

Zero Trust

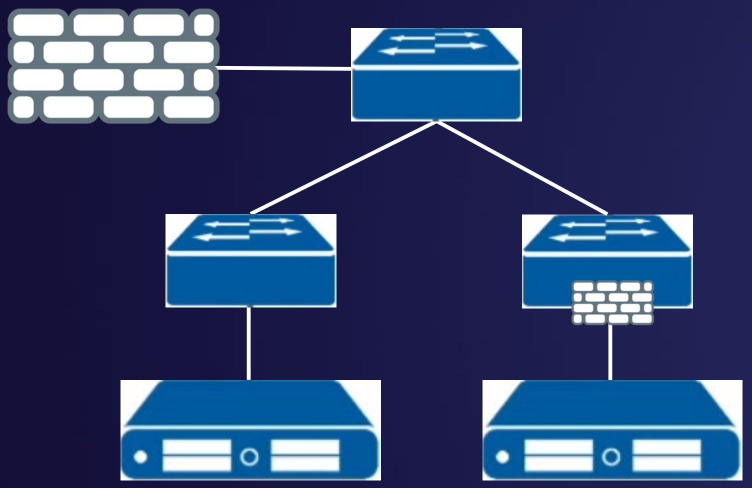
Objects within a network are no more trustworthy than objects outside a network

Secures data and applications with micro-perimeters

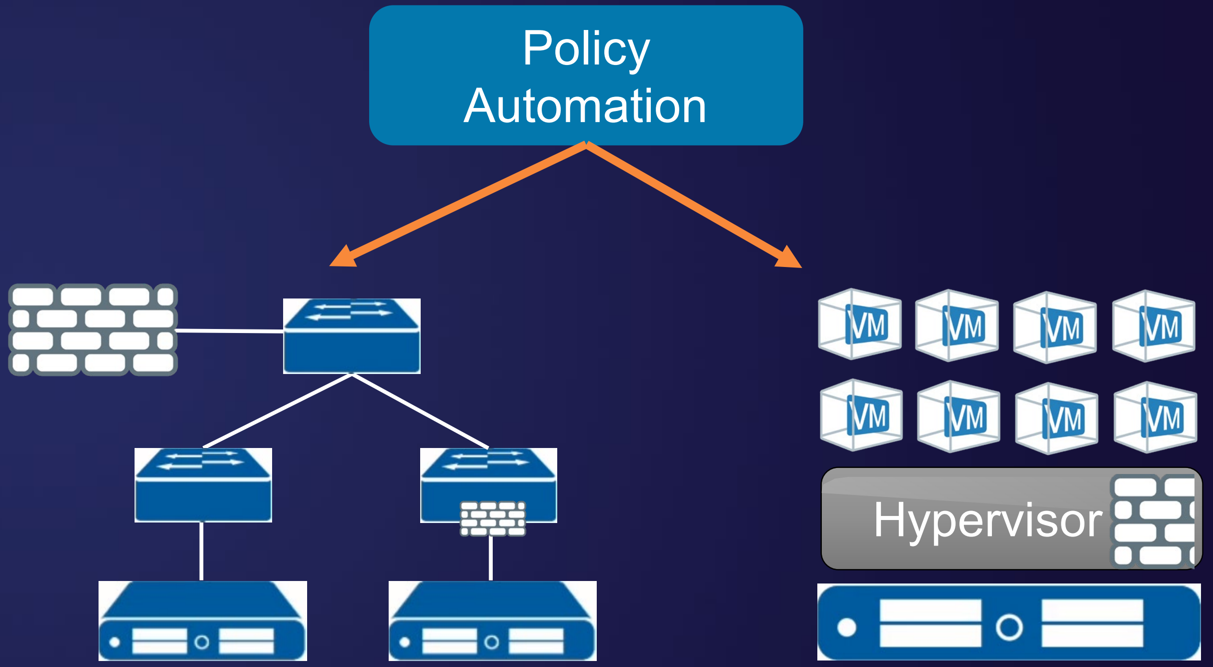
> “Can reduce an organization’s risk exposure by 37% or more.
> Reduce security costs by 31% and realize millions of dollars in savings in their overall IT security budgets.”

Typical Approaches Fall Short

Network Based Segmentation



SDN-Based Segmentation



Policy Automation

Multiple Administration Points
Policy tied to IP-Addresses
Applications often not conveniently located relative to network boundaries

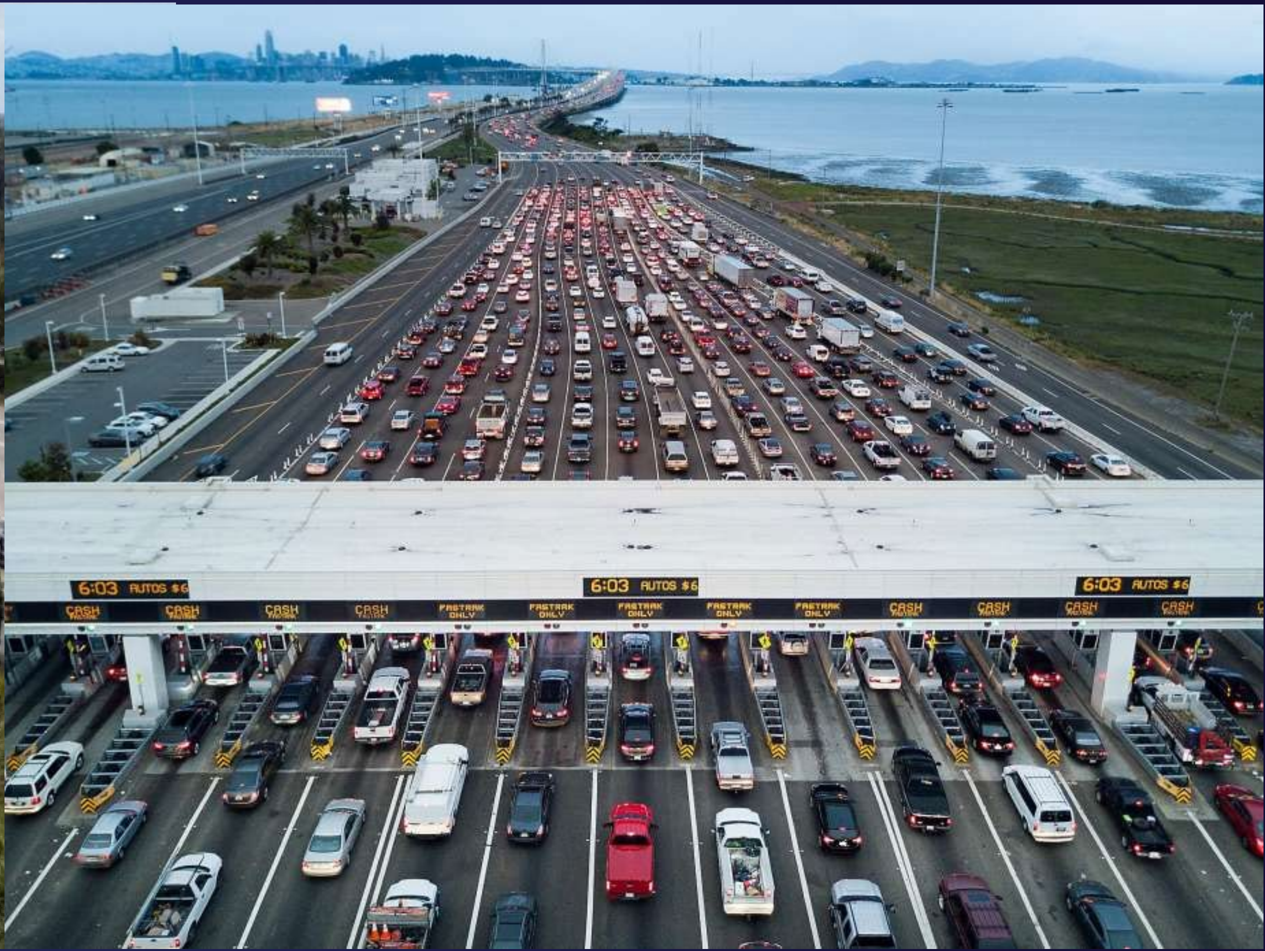
Typical Approaches Fall Short

IMPACT

- **Increased risk** of network and/or applications failing
- **Increased network fragility** (hard to manage)
- **Lower agility** (fear of failure)

Opposing Ideas must Co-Exist

Fast, Flexible, Reliable, Open Connectivity



Isolation and Static Control

illumio

De-coupling …

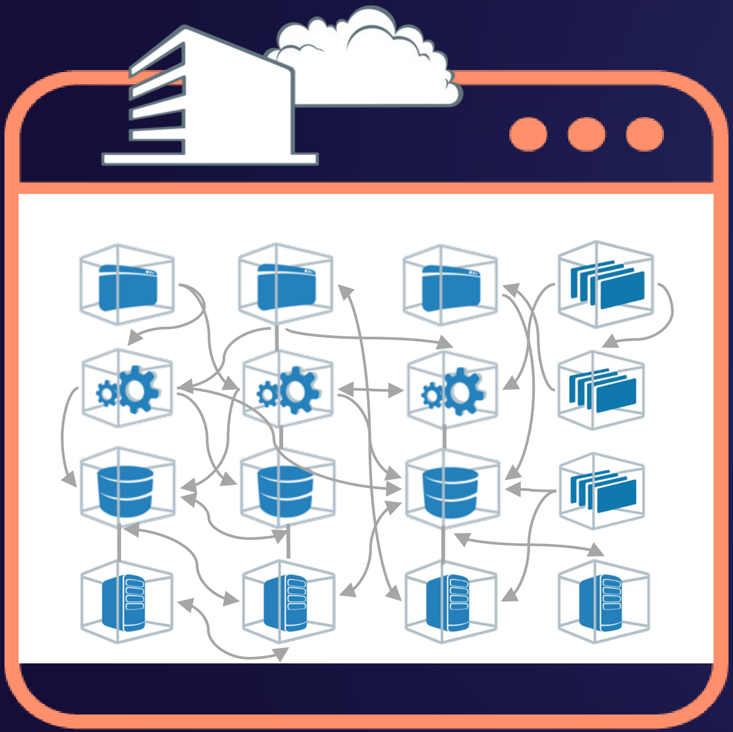
Fast, Flexible, Reliable Connectivity

Collect Fees

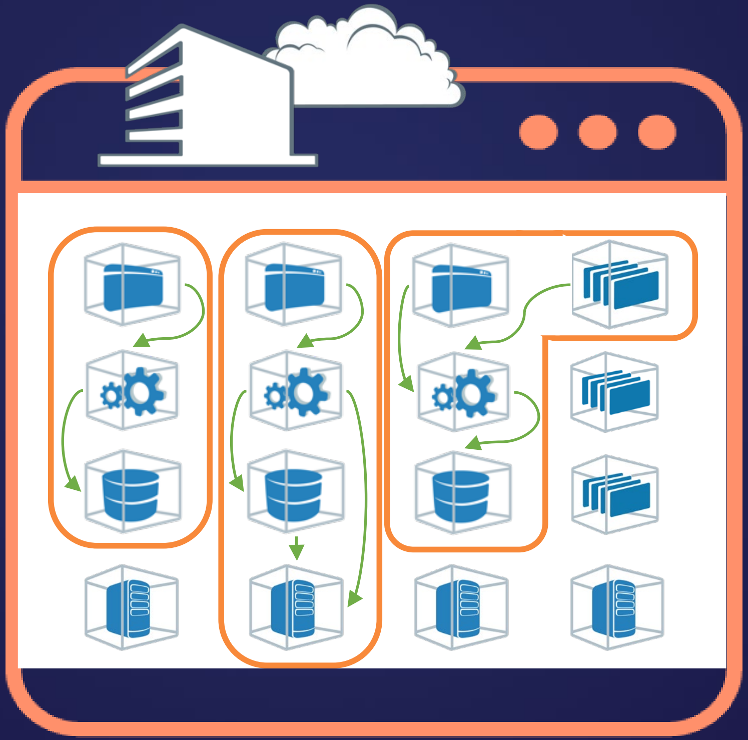
The Only Way to do this

What’s Needed

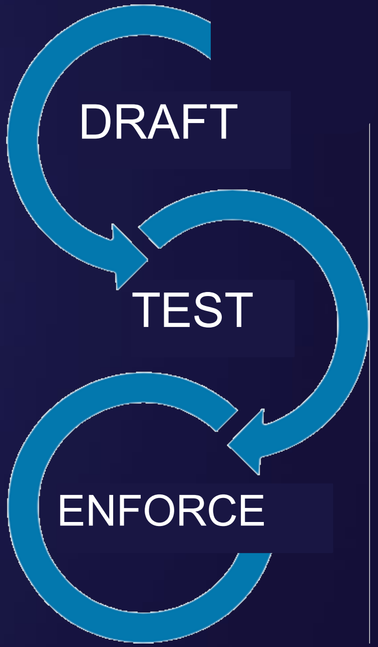
Map of your compute, applications and connectivity



A way to group **logical** bunches of “things”

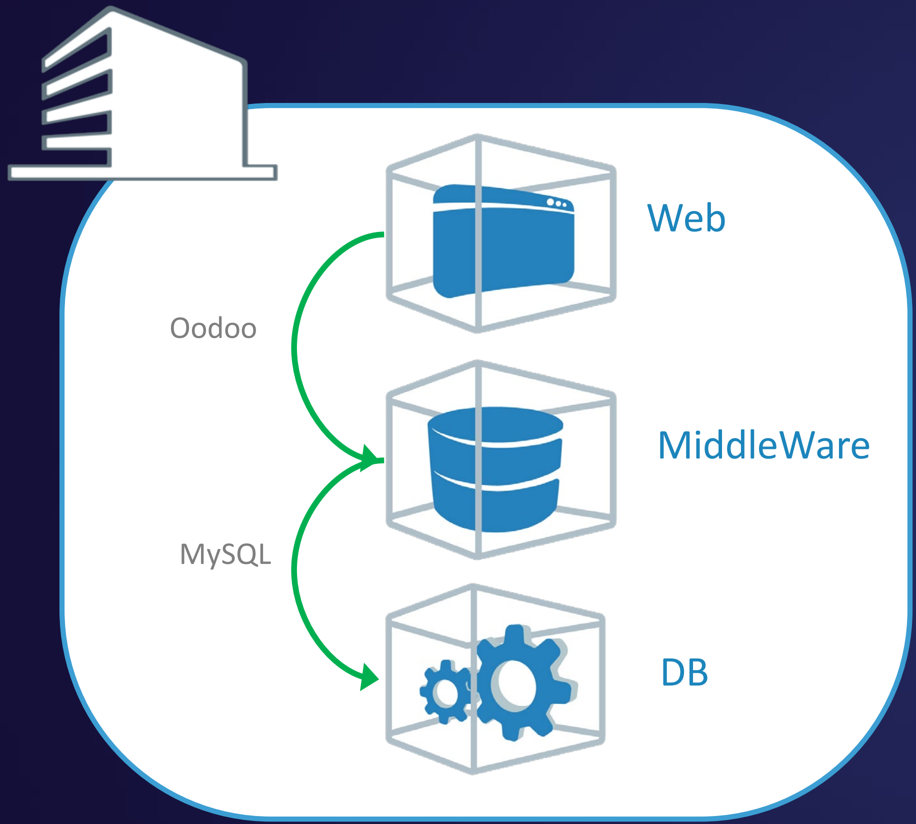


Deploy Security Segmentation **without Network Risk**



illumio

Secured by Design / Intent Example



Records-Mngt : Staging : Equinix

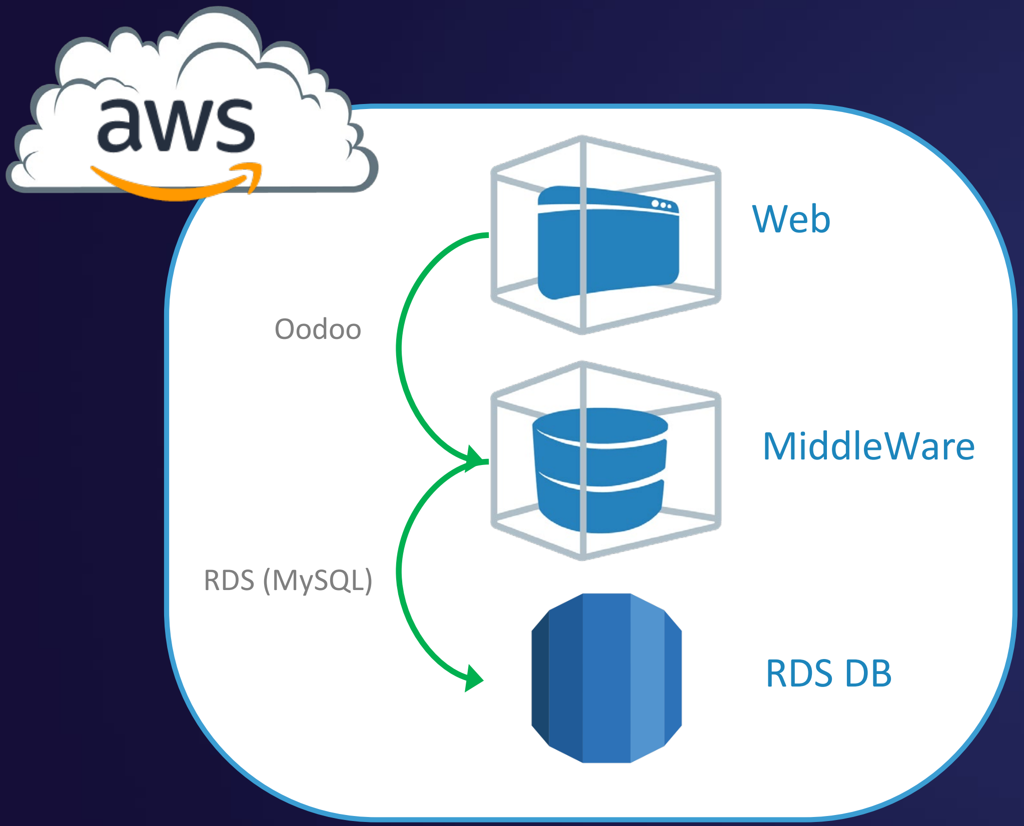
Name
Records-Mngt Policy

Scope
Records-Mngt : Dev-Test : Equinix
Records-Mngt : Staging : Equinix

Rules

Services	Provided By	Used By
Apache	Web	Company HQ
Oodoo	Middleware	Web
MySQL	DB	Middleware

Migrating to Public Cloud



Records-Mngt : Staging : AP-SouthEast-2

Name

Online-Store Policy

Scope

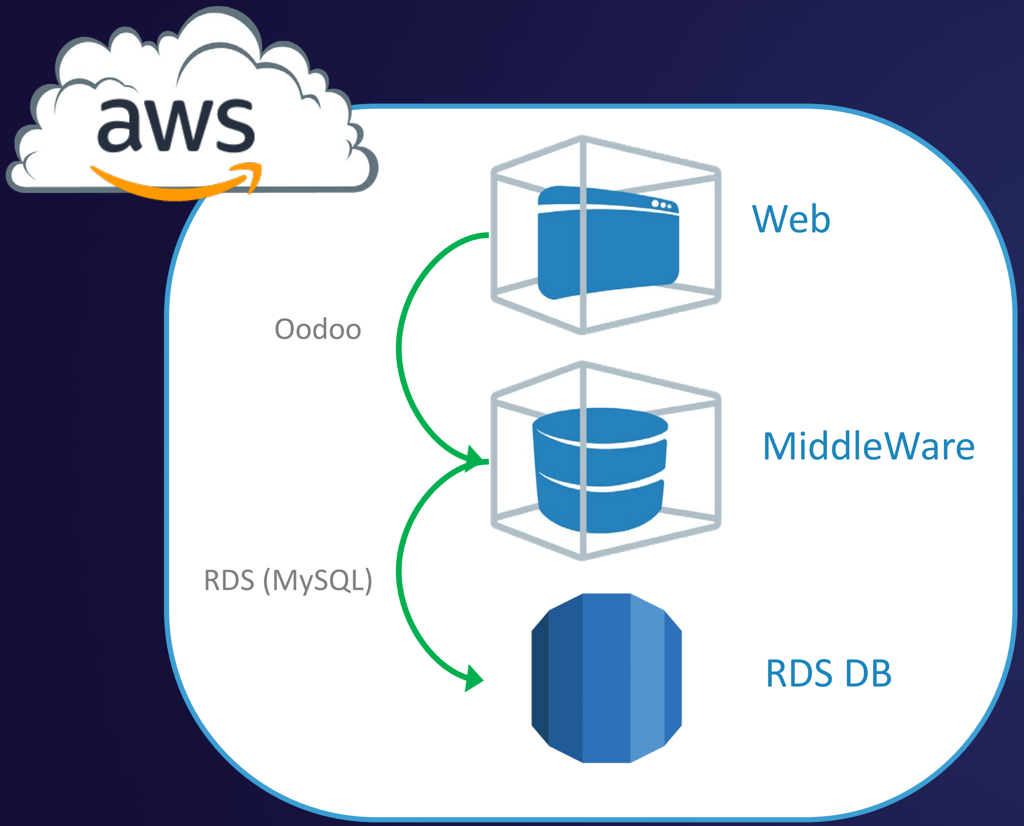
Records-Mngt : Dev-Test : AP-SouthEast-2
Records-Mngt : Staging : AP-SouthEast-2

Rules

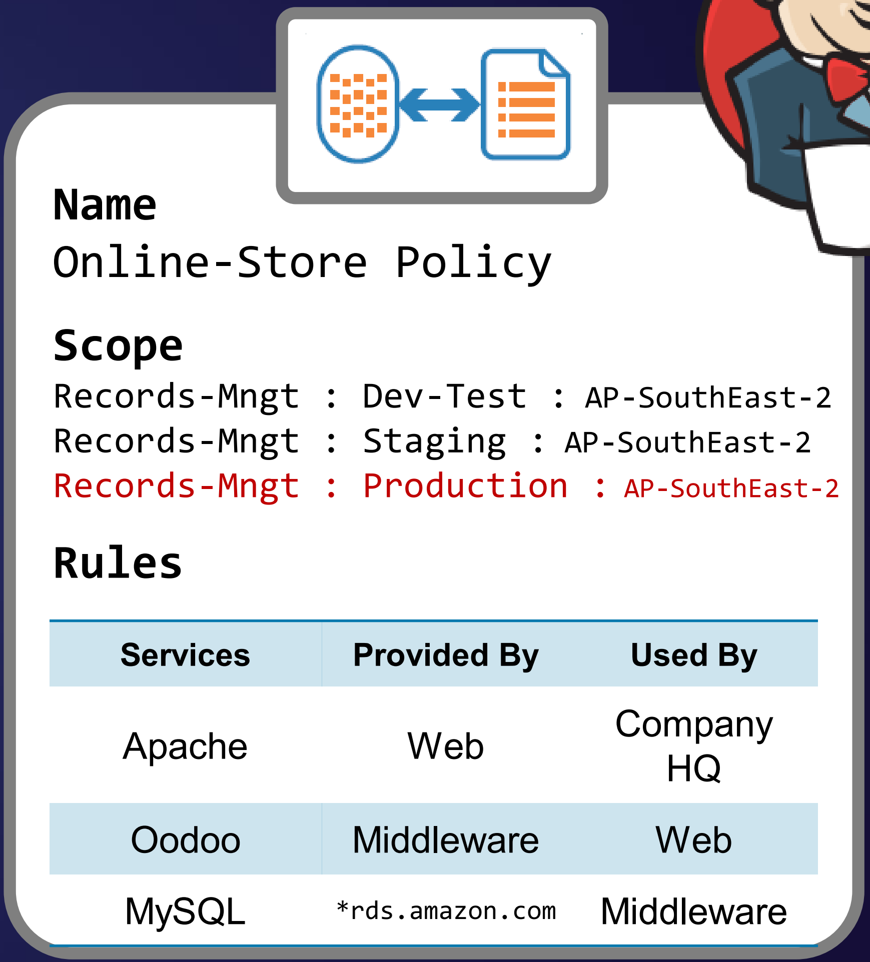
Services	Provided By	Used By
Apache	Web	Company HQ
Oodoo	Middleware	Web
MySQL	*rds.amazon.com	Middleware

illumio

Promoting to Production



Records-Mngt : Production : AP-SouthEast-2



Name

Online-Store Policy

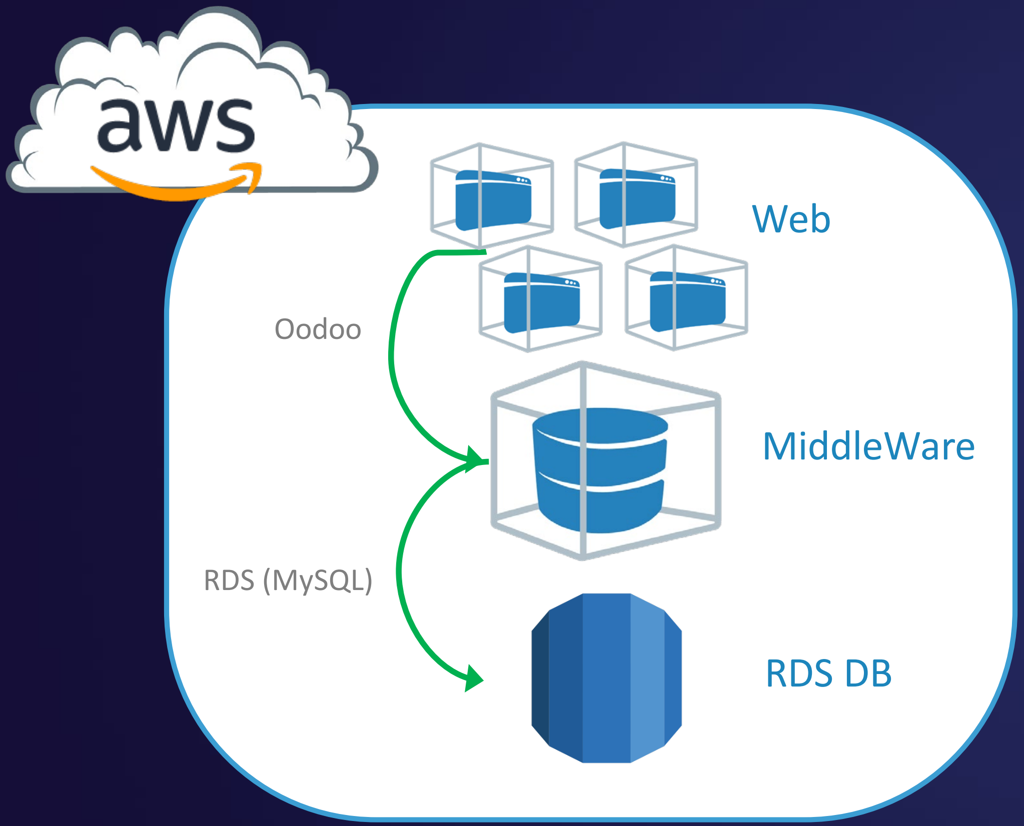
Scope

Records-Mngt : Dev-Test : AP-SouthEast-2
Records-Mngt : Staging : AP-SouthEast-2
Records-Mngt : Production : AP-SouthEast-2

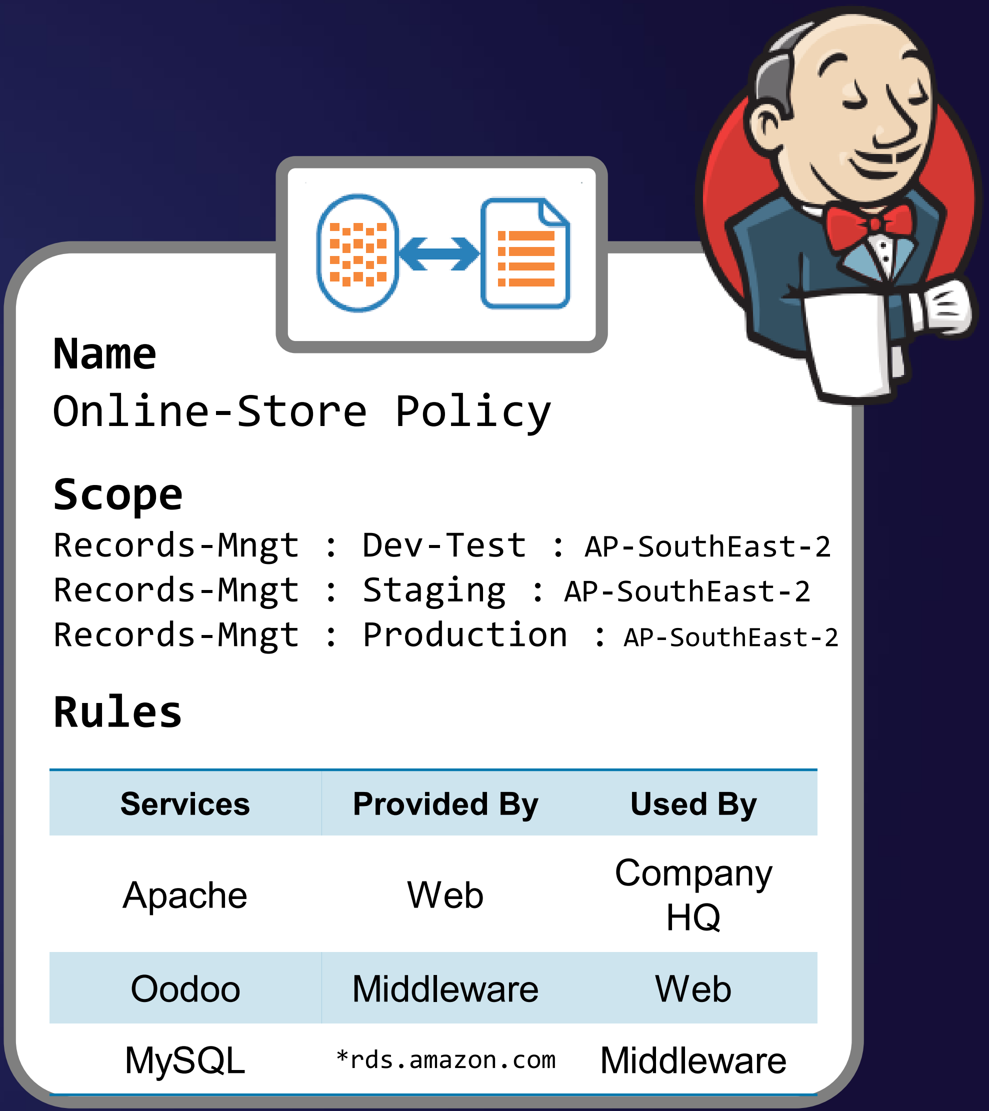
Rules

Services	Provided By	Used By
Apache	Web	Company HQ
Oodoo	Middleware	Web
MySQL	*rds.amazon.com	Middleware

Auto-Scaling in Production



Records-Mngt : Production : AP-SouthEast-2



Name

Online-Store Policy

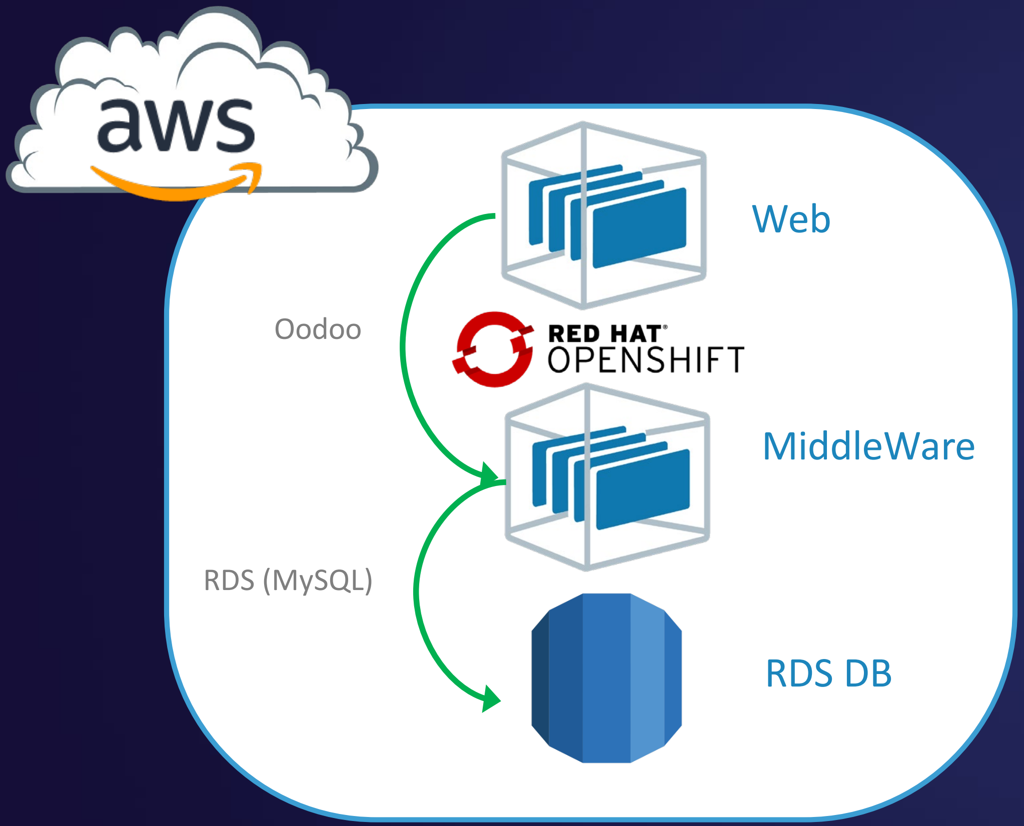
Scope

Records-Mngt : Dev-Test : AP-SouthEast-2
Records-Mngt : Staging : AP-SouthEast-2
Records-Mngt : Production : AP-SouthEast-2

Rules

Services	Provided By	Used By
Apache	Web	Company HQ
Oodoo	Middleware	Web
MySQL	*rds.amazon.com	Middleware

Containerise App



Records-Mngt : Production : AP-SouthEast-2

Name

Online-Store Policy

Scope

```
Records-Mngt : Dev-Test : AP-SouthEast-2
Records-Mngt : Staging : AP-SouthEast-2
Records-Mngt : Production : AP-SouthEast-2
```

Rules

Services	Provided By	Used By
Apache	Web	Company HQ
Oodoo	Middleware	Web
MySQL	*rds.amazon.com	Middleware

illumio

Segmentation Operation

NETWORKING

Connectivity, Resilience & Performance

De-couple security from the network fabric

INFRASTRUCTURE

Workload operations, performance & agility

Automate s/w deployment and/or Golden Images

APPLICATIONS

Meet Business Needs, speed of delivery without compromising security

----

Author Security Policy relevant to their application(s)

SECURITY

Maintain Security Strategy, Governance & operate SOC

Approve & Provision Application Security Policies & Take Action

illumio

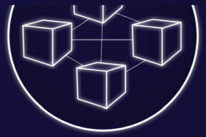
Practical Steps to Zero Trust

1 Identify high-value systems and visualise relations and connections in real time

2 Architect optimal micro-segmentation strategy, visualise and test policies before enforcement

3 Default-deny model applying enforcement for each workload

4 Automate and adapt to change whilst orchestrating security incident response



THANKS!

illumio