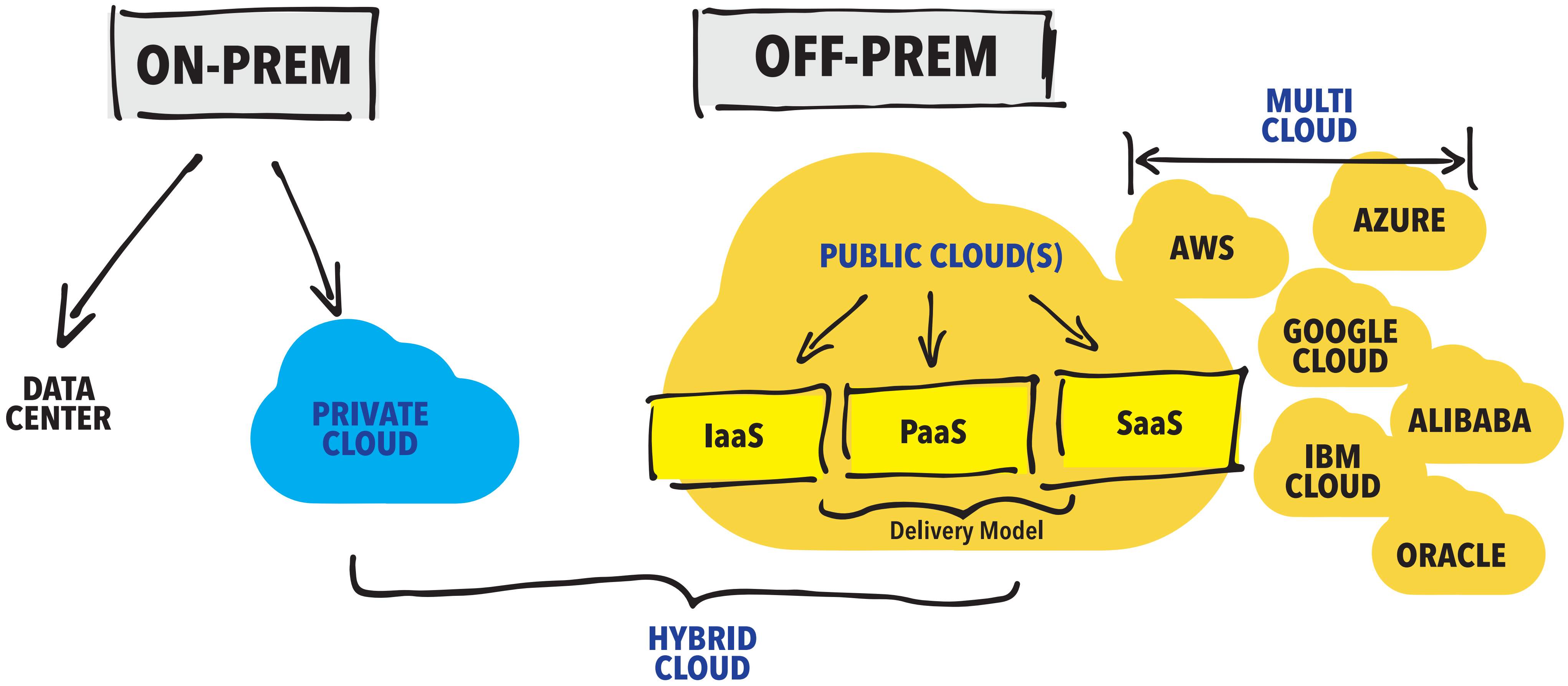
Continuous Compliance

Borna Cisar

AVANTEC
Competence. Security. Trust.



ON-PREM

DATA CENTER

PRIVATE CLOUD

OFF-PREM

PUBLIC CLOUD(S)

IaaS

PaaS

SaaS

Delivery Model

MULTI CLOUD

AWS

AZURE

GOOGLE CLOUD

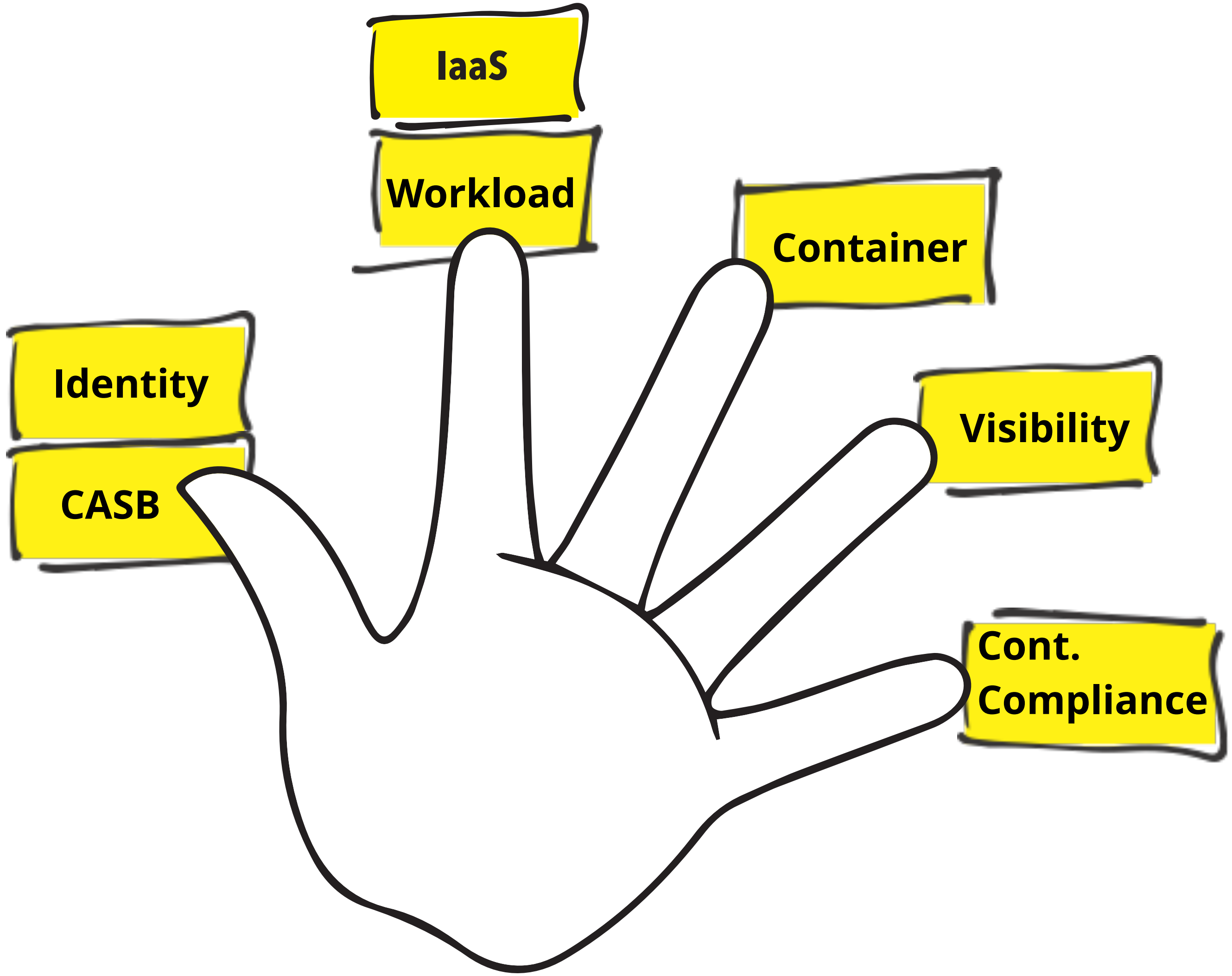
ALIBABA

IBM CLOUD

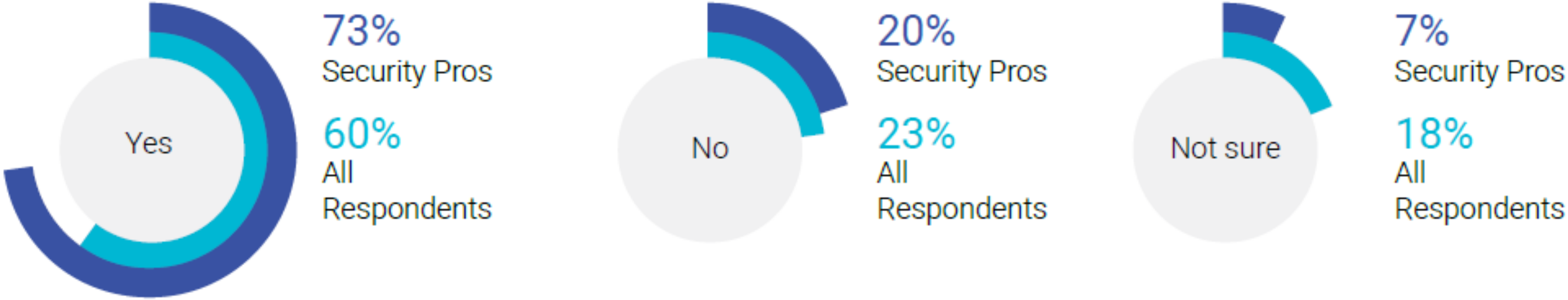
ORACLE

HYBRID CLOUD

Where are we, so far?

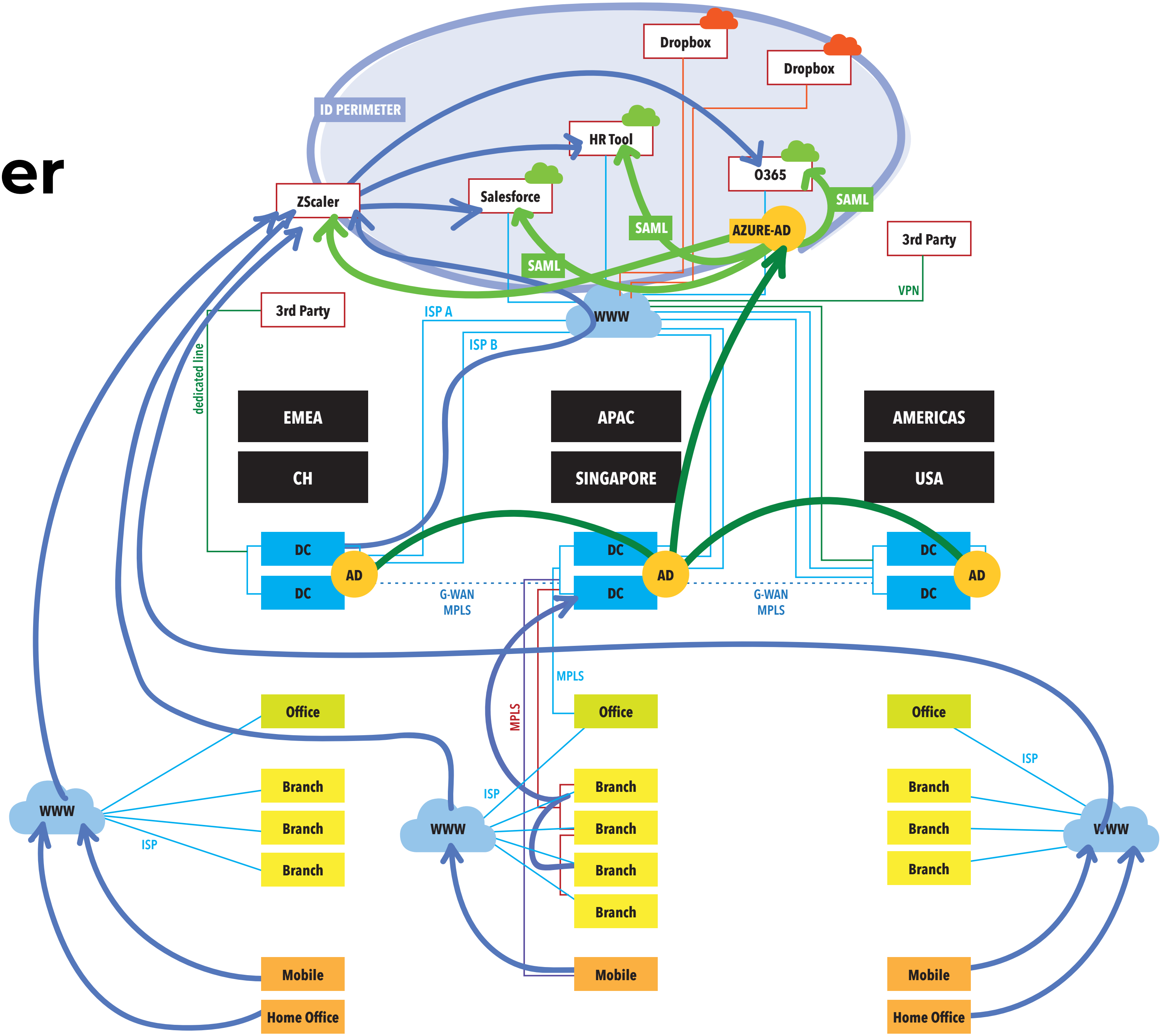


Does your org need to **manually** configure security policies for Applications in the Cloud?

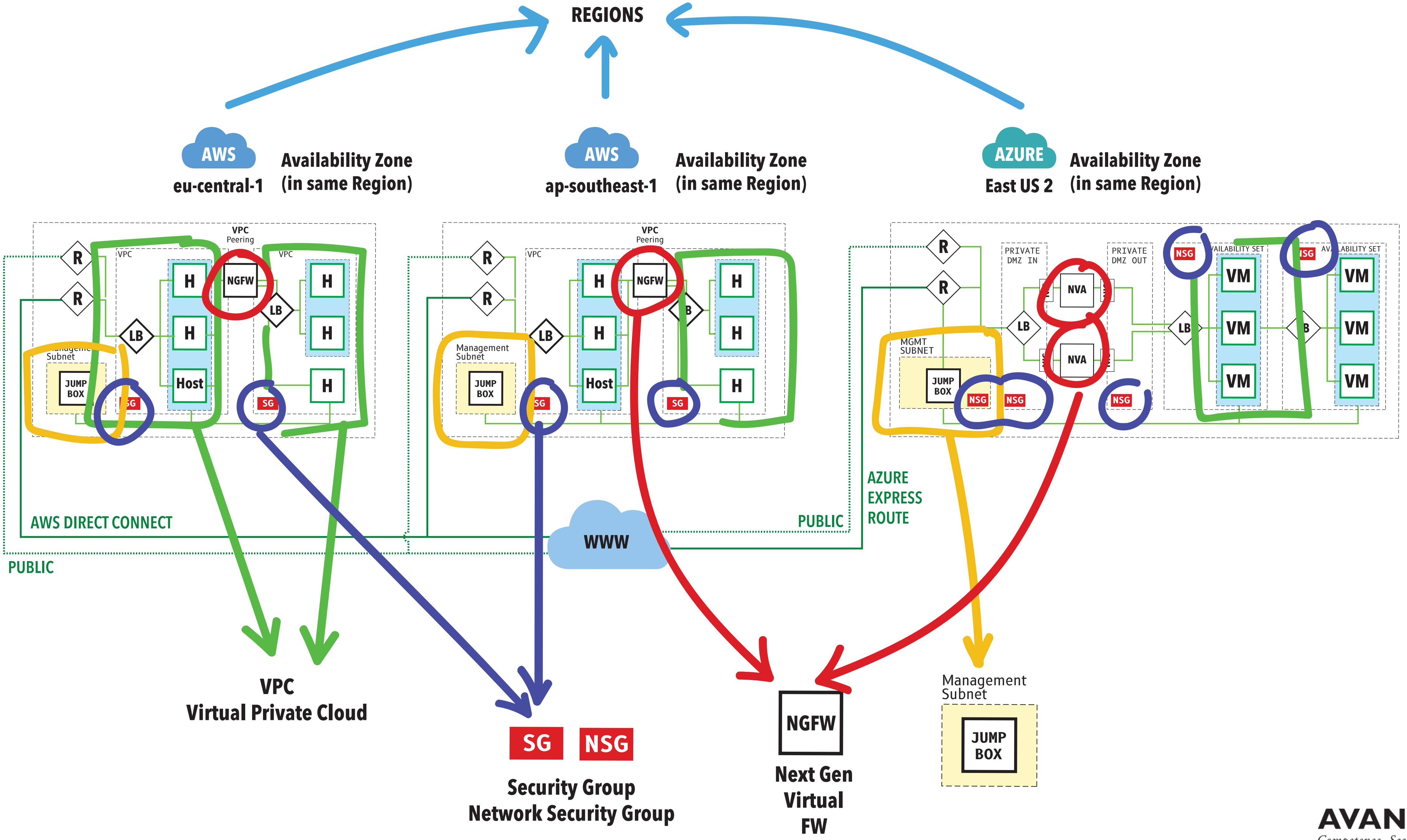


2018 Report: State of Securing Cloud Workloads

Identity Perimeter And CASB



AVANTEC
Competence. Security. Trust.

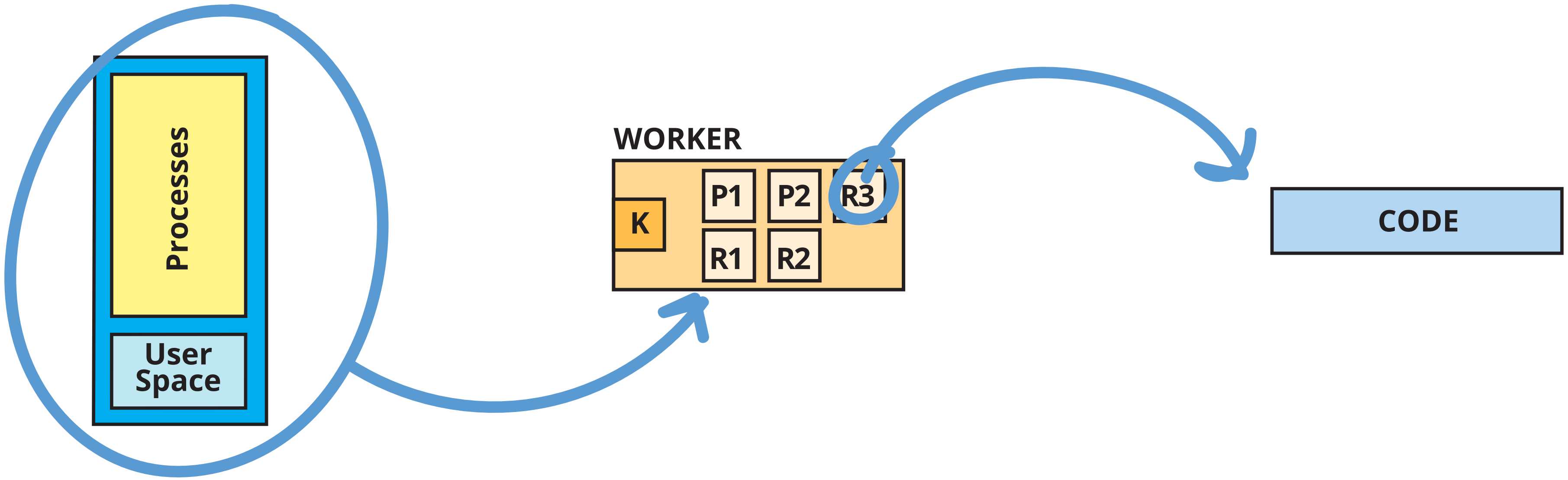


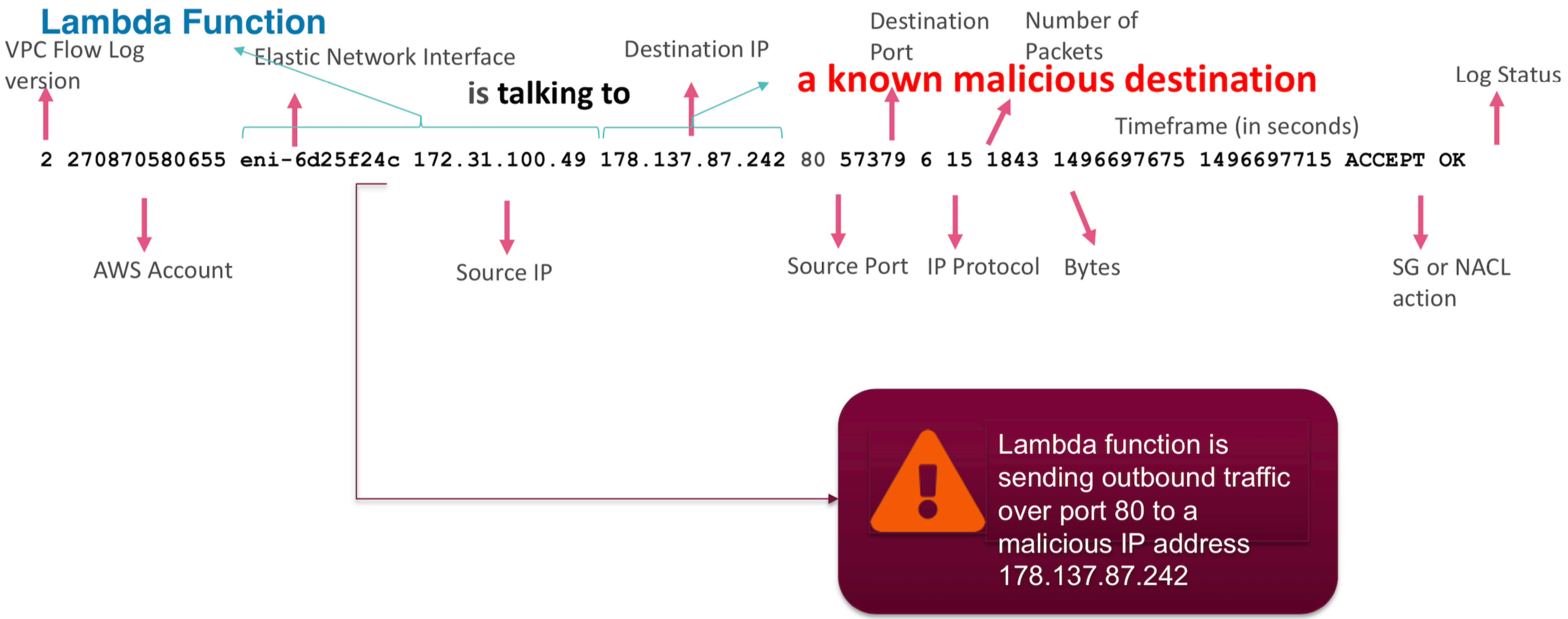
AVANTEC
Competence. Security. Trust.

Container

Kubernetes

Serverless





Lambda Function is talking to **a known malicious destination**

VPC Flow Log version

Elastic Network Interface

Destination IP

Destination Port

Number of Packets

Log Status

Timeframe (in seconds)

```
2 270870580655 eni-6d25f24c 172.31.100.49 178.137.87.242 80 57379 6 15 1843 1496697675 1496697715 ACCEPT OK
```

AWS Account

Source IP

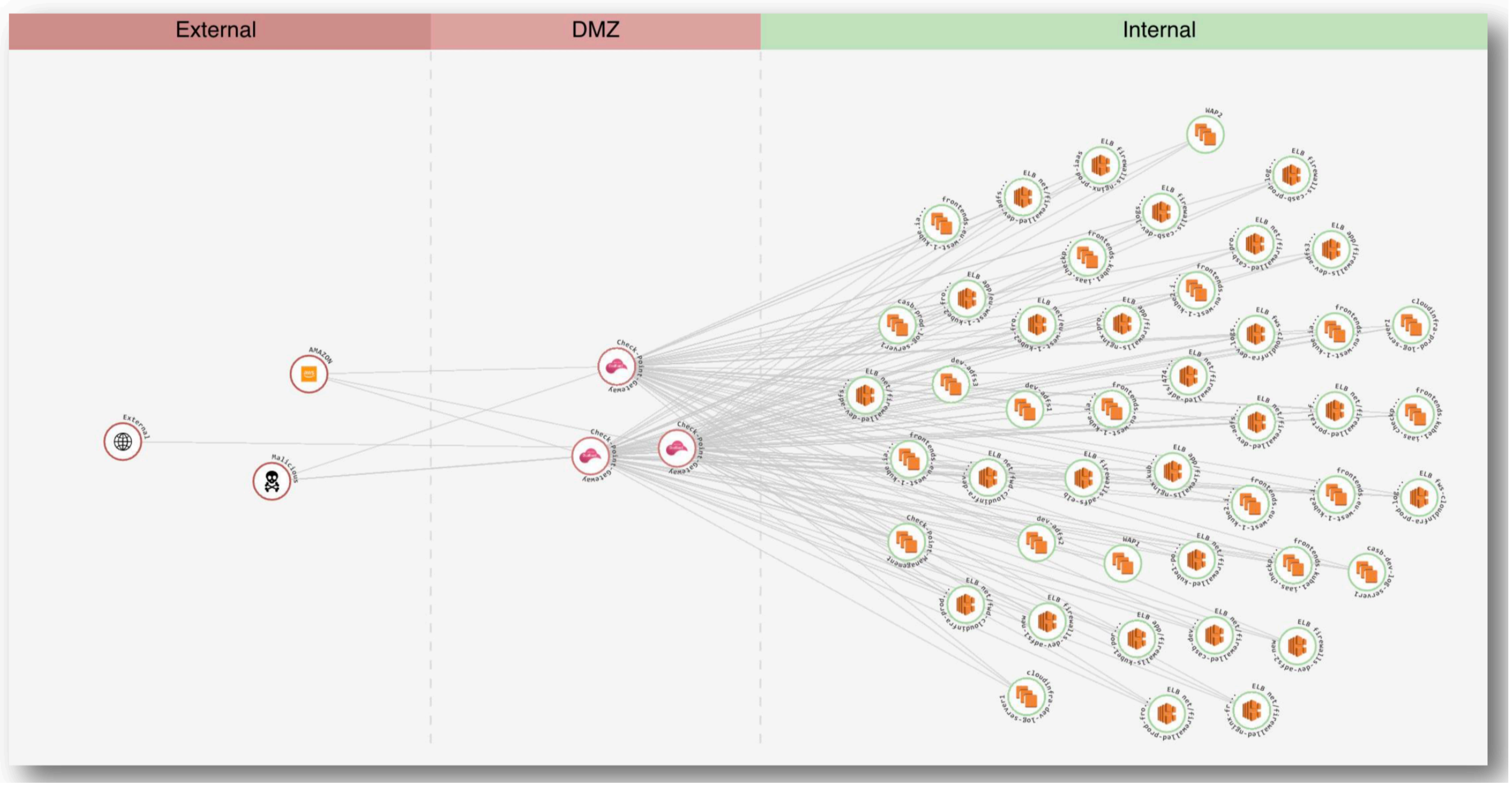
Source Port

IP Protocol

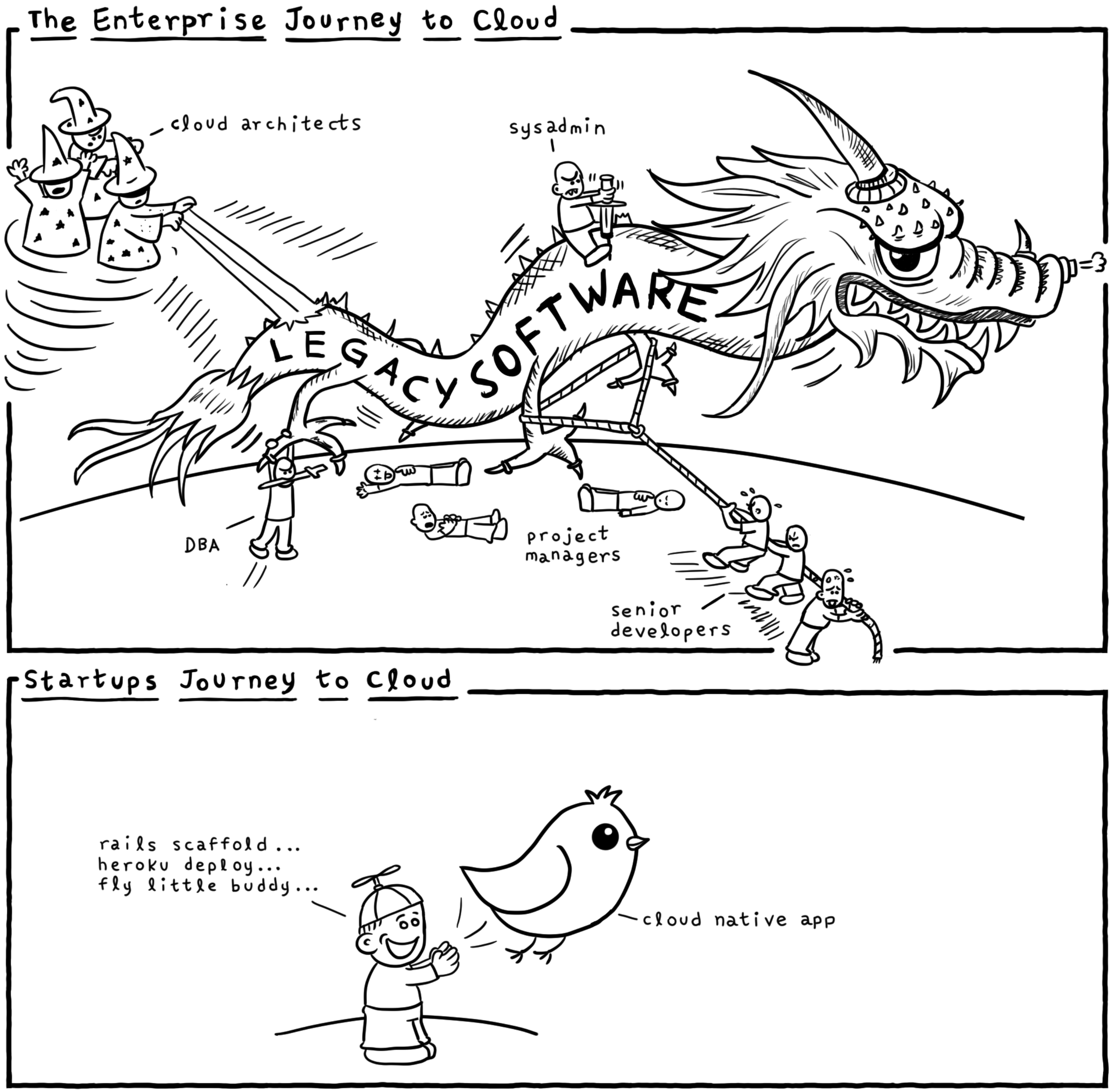
Bytes

SG or NACL action

Lambda function is sending outbound traffic over port 80 to a malicious IP address 178.137.87.242


External
DMZ
Internal
External
AMAZON
Malicious
Check-Point-Gateway
Check-Point-Gateway
Check-Point-Gateway
WAP2
ELB firewalls-nginx-prod-iaas
ELB net/firewalled-dev-adfs...
frontends.eu-west-1-kube.ia...
ELB firewalls-casb-prod-log...
ELB firewalls-casb-dev-logs...
frontends.kube1.iaas.checkp...
ELB net/firewalled-casb-pro...
ELB app/firewalls-dev-adfs3...
ELB app/eu-west-1-kube2-fro...
frontends.eu-west-1-kube2.i...
casb-prod-log-server1
ELB net/eu-west-1-kube2-fro...
ELB app/firewalls-nginx-pro...
ELB fws-cloudinfra-dev-logs...
frontends.eu-west-1-kube.ia...
cloudinfra-prod-log-server1
ELB net/firewalled-dev-adfs...
dev-adfs3
ELB net/firewalled-adfs|474...
dev-adfs1
frontends.eu-west-1-kube.ia...
ELB net/firewalled-dev-adfs...
ELB net/firewalled-portal-f...
frontends.kube1.iaas.checkp...
frontends.eu-west-1-kube.ia...
ELB net/fwd-cloudinfra-dev-...
ELB firewalls-adfs-elb
ELB app/firewalls-nginx-kub...
frontends.eu-west-1-kube2.i...
frontends.eu-west-1-kube2.i...
ELB fws-cloudinfra-prod-log...
Check-Point-Management
dev-adfs2
WAP1
ELB net/firewalled-kube1-po...
frontends.kube1.iaas.checkp...
casb-dev-log-server1
ELB net/fwd-cloudinfra-prod...
ELB firewalls-dev-adfs1-nau
ELB app/firewalls-kube1-pod...
ELB net/firewalled-casb-dev...
ELB firewalls-dev-adfs2-nau
cloudinfra-dev-log-server1
ELB net/firewalled-prod-fro...
ELB net/firewalled-nginx-fr...

How shall we handle all of this?



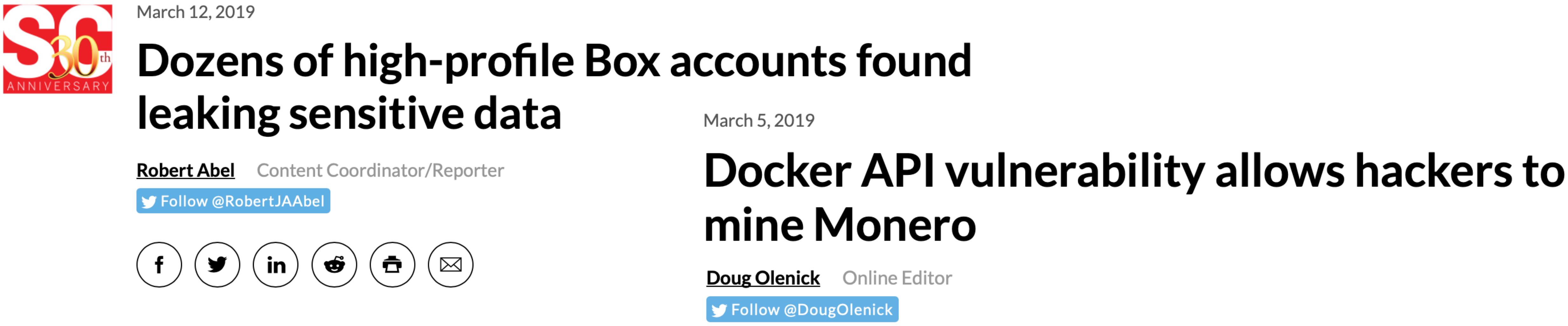
Daniel Stori {turnoff.us}
Thanks to Michael Tharrington

How will we handle all of this?

That’s where the strength of the Cloud Native approach lies.

Look at the “Control Plane” of the cloud.

How will we handle all of this?



March 12, 2019

Dozens of high-profile Box accounts found leaking sensitive data

Robert Abel Content Coordinator/Reporter

Follow @RobertJAAbel

March 5, 2019

Docker API vulnerability allows hackers to mine Monero

Doug Olenick Online Editor

Follow @DougOlenick

Exposed Docker hosts can be exploited for cryptojacking attacks

Charlie Osborne 3/5/2019

How will we handle all of this?

VISIBILITY

- Assets
- Applications
- Network

- Security Posture

CONTINUOUS COMPLIANCE

- Continually assess the state of your assets, applications and infrastructure

- Enforce best-practices and automatically correct against security standards

Platform

- Add Scanning
- Add threat intelligence

Developers

CI/CD Pipeline

Security shifting “Left”

But are you prepared?

Can you secure “at cloud speed”?

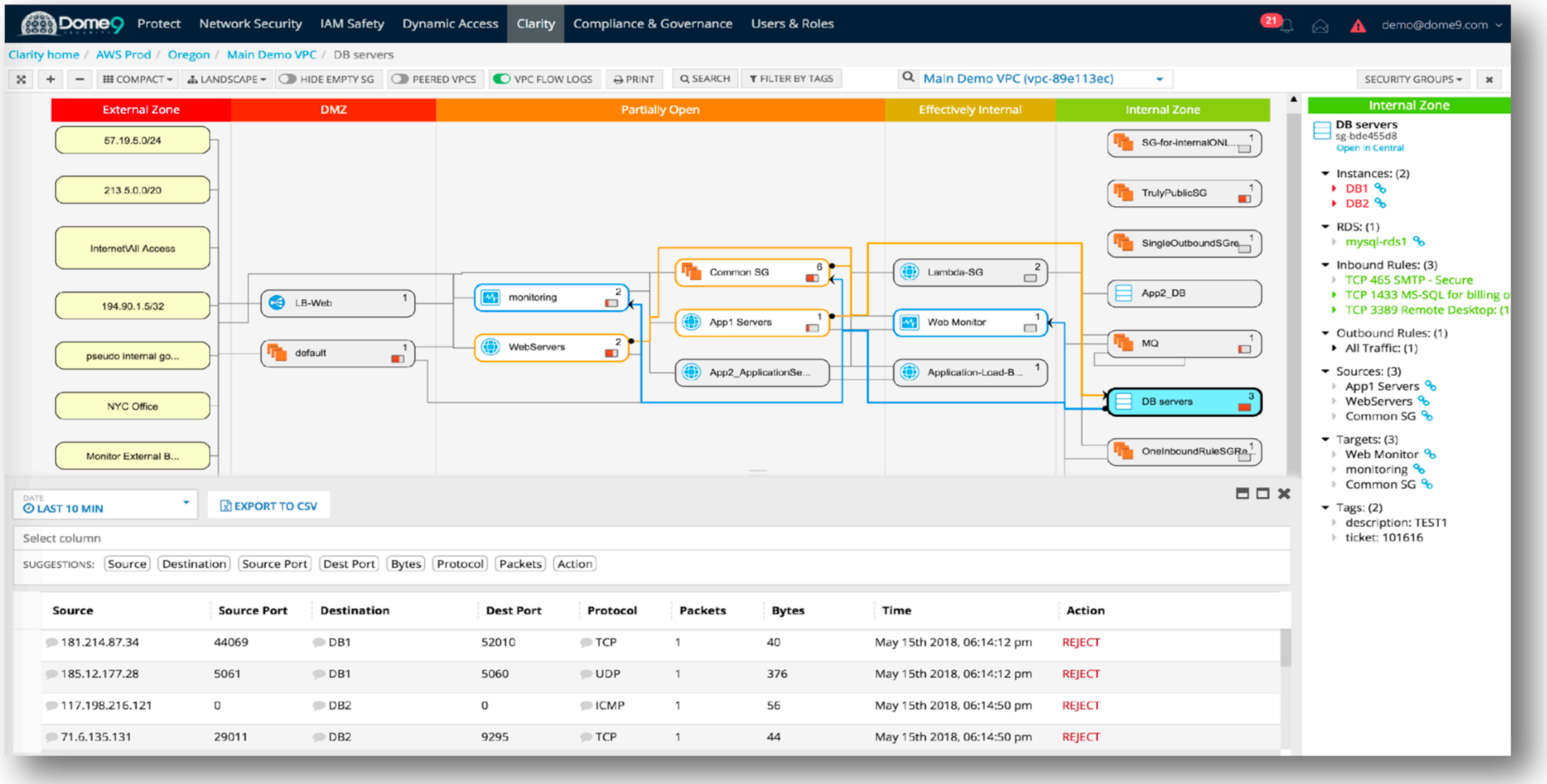
Can you integrate with code?

Continuous Compliance

= Continuous Security*

* Oversimplification for the sake of the presentation

Visibility



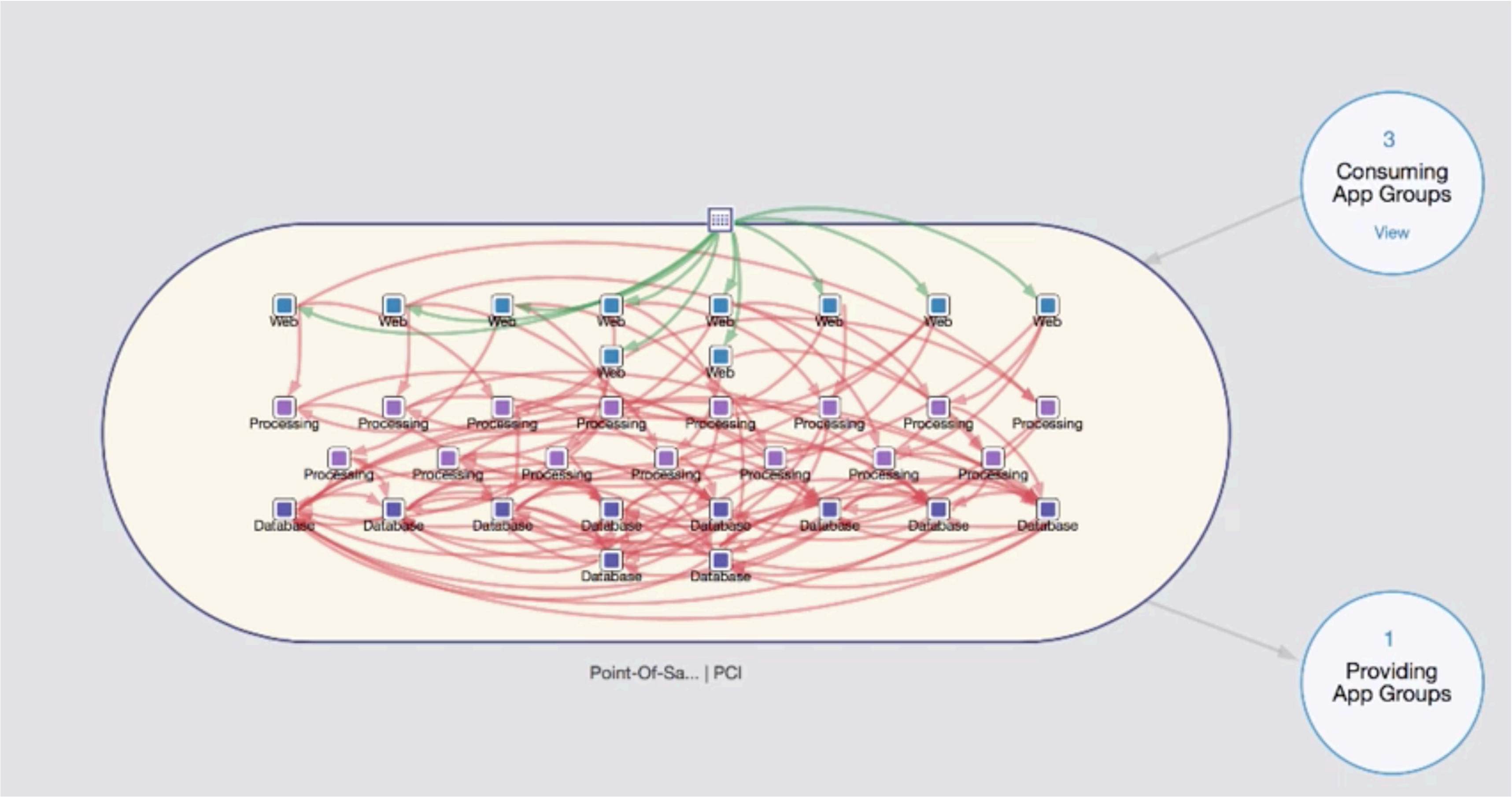
Internal Zone

DB servers
sg-bde455d8
Open in Central

- Instances: (2)
  - DB1
  - DB2
- RDS: (1)
  - mysql-rds1
- Inbound Rules: (3)
  - TCP 465 SMTP - Secure
  - TCP 1433 MS-SQL for billing o
  - TCP 3389 Remote Desktop: (1
- Outbound Rules: (1)
  - All Traffic: (1)
- Sources: (3)
  - App1 Servers
  - WebServers
  - Common SG
- Targets: (3)
  - Web Monitor
  - monitoring
  - Common SG
- Tags: (2)
  - description: TEST1
  - ticket: 101616

Source	Source Port	Destination	Dest Port	Protocol	Packets	Bytes	Time	Action
181.214.87.34	44069	DB1	52010	TCP	1	40	May 15th 2018, 06:14:12 pm	REJECT
185.12.177.28	5061	DB1	5060	UDP	1	376	May 15th 2018, 06:14:12 pm	REJECT
117.198.216.121	0	DB2	0	ICMP	1	56	May 15th 2018, 06:14:50 pm	REJECT
71.6.135.131	29011	DB2	9295	TCP	1	44	May 15th 2018, 06:14:50 pm	REJECT

Visibility



AVANTEC
Competence. Security. Trust.

Automatic discovery
(Assets are tagged)

Compliance
Against standards

Auto-remediation
Desired state-management

Enforcement
(automatic enforcement)

On all platforms

Identity

CASB

IaaS

Workload

Containers

Kubernetes

Serverless

**Enable declarative
Security**

**Automate policies through
Scripting language**

**Work with
The developers**

DevSecOps

Leverage strength of Cloud-native

Understand your organisations Security posture

Work continuously and Automatically on security

Remember that...

“Through 2020, **95%** of cloud security failures will be the **custo** **ult.**”

Gartner

NOT ANYMORE!

Thanks for your time

AVANTEC
Competence. Security. Trust.