RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

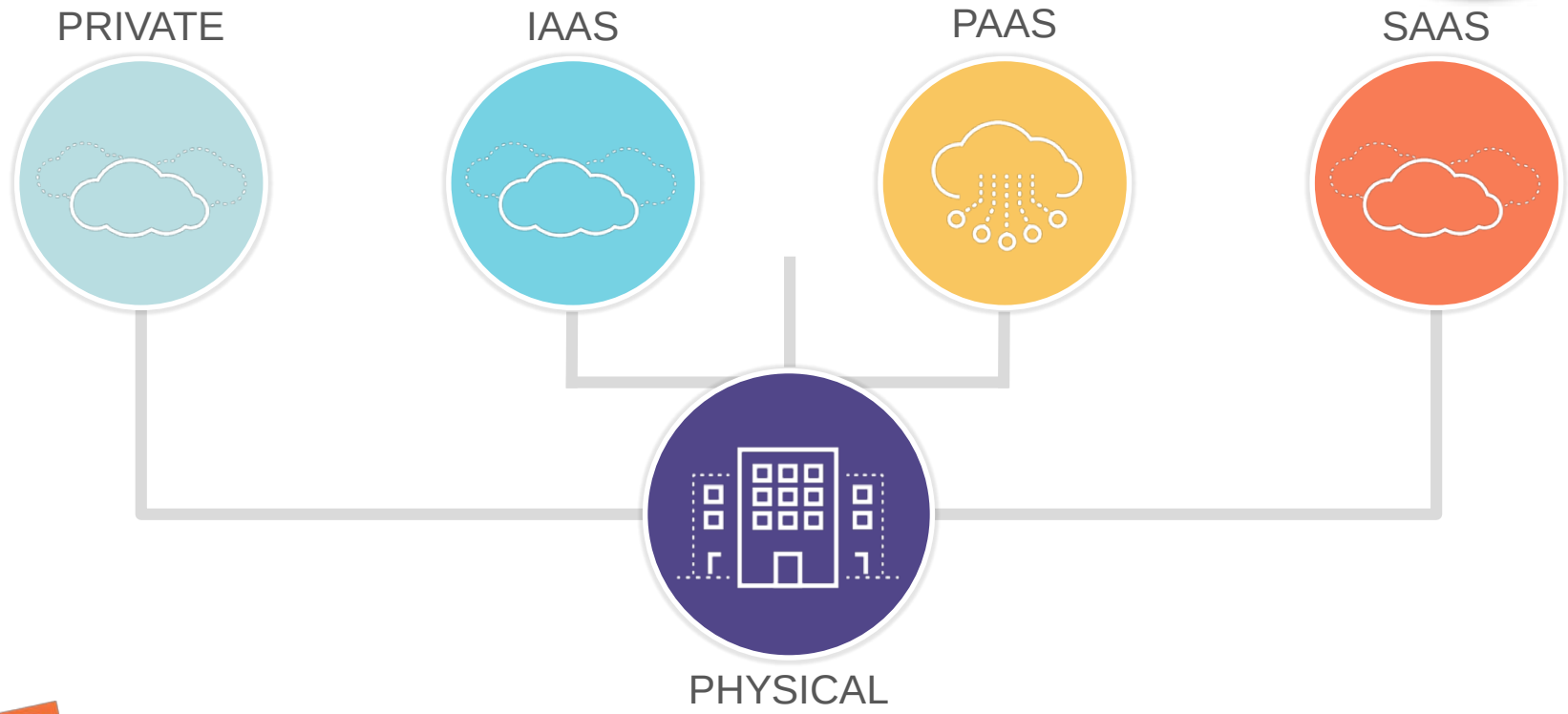
SESSION ID: **SPO3-W14**

IS CLOUD NATIVE SECURITY GOOD ENOUGH?

JANET MATSUDA
SENIOR VICE PRESIDENT
PALO ALTO NETWORKS

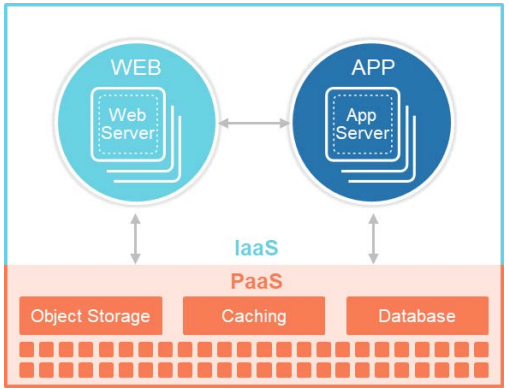
TIM PRENDERGAST
CHIEF CLOUD OFFICER
PALO ALTO NETWORKS

DATA AND APPLICATIONS ARE EVERYWHERE

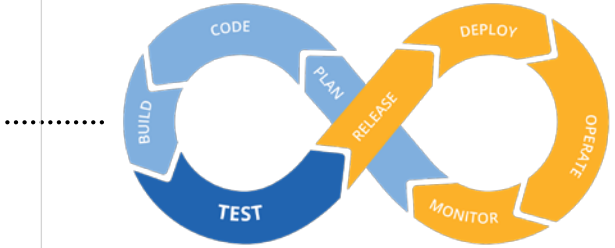


But I'm not in the cloud…

RAPID DEPLOYMENT ACROSS CLOUDS



DEVELOPED FOR CLOUD



DEPLOYED FOR SPEED

MANAGED ACROSS CLOUDS

NO SHORTAGE OF SERVICES

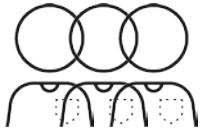
CLOUD ADOPTION MATURITY

EXPLORE

IMPLEMENT

OPTIMIZE

DIFFERENT TEAM PERSPECTIVES ON RISK



Application Team

Integrity and resiliency of the application

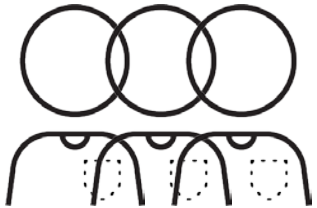
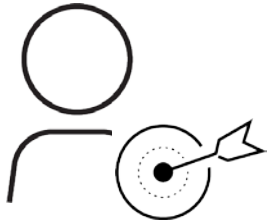
InfoSec Team

Risk of exposure to data breaches and cyberattacks.
Quantify and measure risk around applications in cloud

CXO

Maintain our commitments to our stakeholders (Board, regulatory, partners, customer)

LACK OF VISIBILITY CREATES RISK

I have no visibility.	Did that really just happen?	Nothing's changed, has it?	I'm not sure our policies are relevant.	I can't sleep because I just don't know …
				
SECOPS	DEVOPS	RISK & COMPLIANCE	CISO	CXO

SECURITY AUTOMATION PROVIDES CLARITY

REAL-TIME DISCOVERY

CONTINUOUS MONITORING

FLEXIBLE ENGINE

VALIDATES *YOUR* SECURITY POLICY

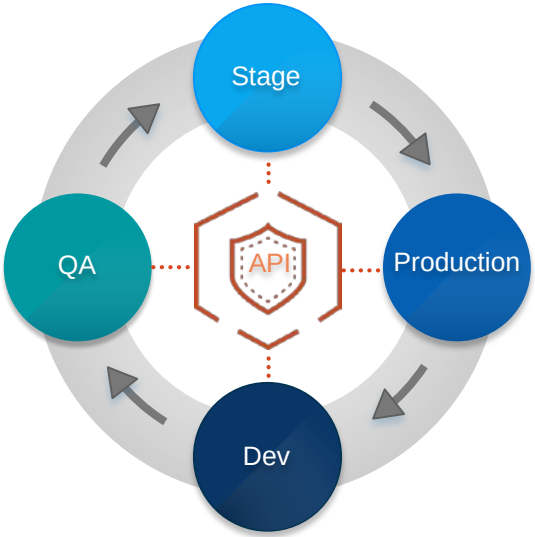
AUTOMATED ACTION

FIX ISSUES BEFORE BAD GUYS FIND THEM

ROBUST REPORTING

DEMONSTRATE SUCCESS & COMPLIANCE

AN API APPROACH TOWARDS SECURITY: DEVOPS WITH GUARDRAILS



- Is MFA Enabled?
- Is any sensitive data exposed?
- What services are running?
- Who has access to this resource?

DISCOVER AND MONITOR RESOURCES

ENFORCE CONSISTENT POLICIES

CONTINUOUSLY MONITOR COMPLIANCE

FAST 4 - RISKS DETECTED WITH VISIBILITY

Insecure VPC

58%

Poor password policy

55%

MFA not enabled

48%

Unprotected root

29%

SECURITY POLICY AS CODE

Policy:
Ensure the default security group restricts all traffic

VPC default security group initial settings:

- Deny all inbound traffic
- Allow all outbound traffic between instances assigned to the security group

If you don't specify a security group the new instance is automatically assigned to this default group.

```
def perform(aws)
      aws.ec2.describe_security_groups.security_groups.each.do [sg]
group_name = sg[group.name]
        if group_name == "default'   group_id = sg[:group_id]
        set_data (group_id:group_id, group_name:group_name,sg:sg)
        if sg[:ip_permissions].empty? && sg[:ip_permissions_egress].empty?
              pass(message:"Default security group'#{group_id}' restrings all
traffic.",resource_id:group_id)
        else
          fail(message:"Default security group'#{group_id}'restricts all
traffic.",resource_id:group_id)
          end
        end
end
```

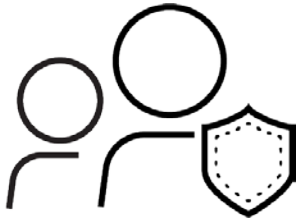
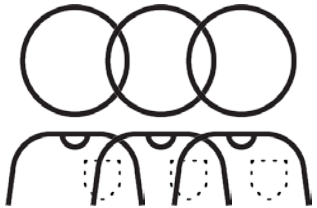
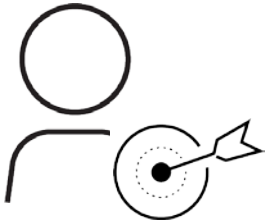
POLICY ENFORCEMENT AS CODE

Control:
PCI DSS 3.21.2.1
Restrict inbound and outbound traffic

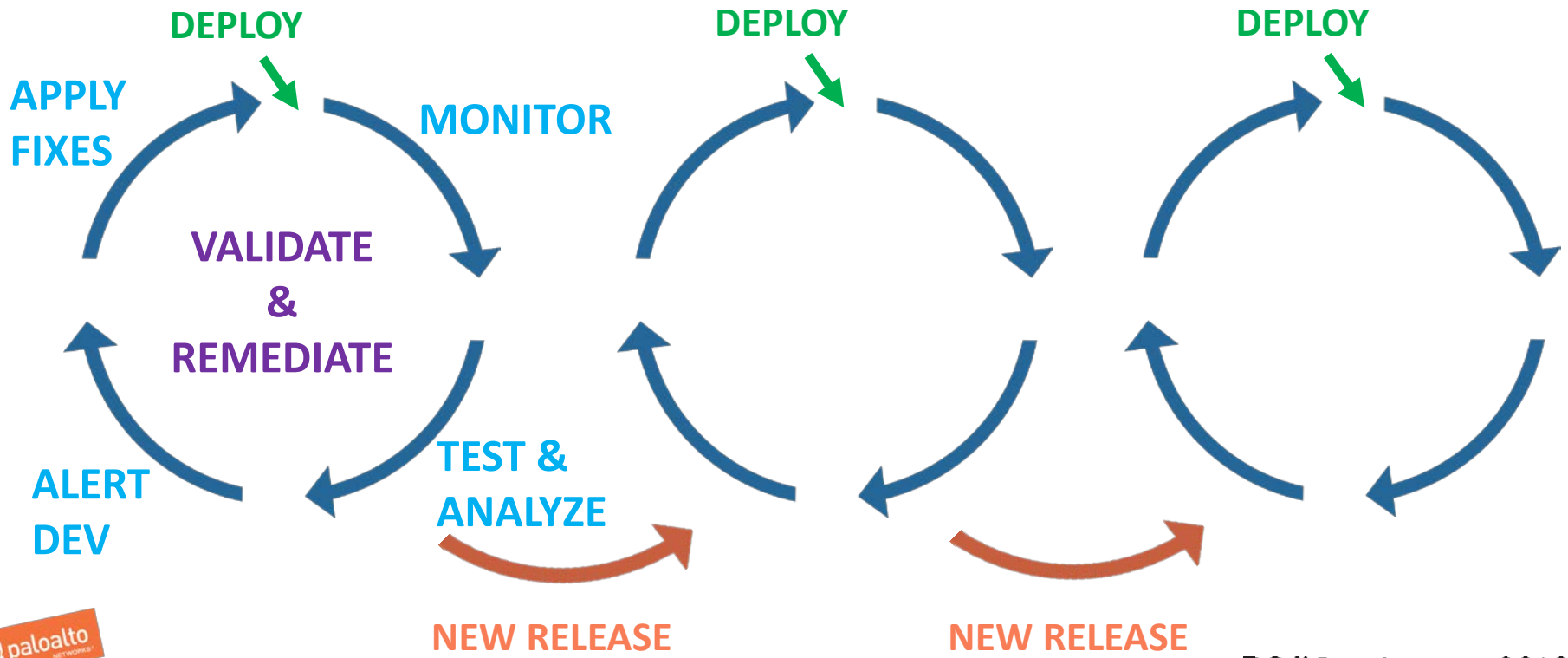
Description:
Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.

```
for admin_port in admin_port_list:
        proto = re.split('-', admin_port)[0]
        port  = re.split('-', admin_port)[1]

        find_port='true' if from_port <= int(port) <= to_port else 'false'

        if cidr_ip in global_cidr_list and ip_protocol.lower() == proto and find_port
== 'true':
            try:
                ec2.revoke_security_group_ingress(GroupId=sg_id, IpPermissions=[
{'IpProtocol': ip_protocol, 'FromPort': from_port, 'ToPort': to_port, IpRanges: [{
IpCidr: cidr_ip }] } ])
            except Exception as e:
                error = str(e.message)
                if 'rule does not exist' not in error:
                    print('=> Error: ', error)
            else:
                print("=> Revoked rule permitting %s/%d-%d with cidr %s from %s" %
(ip_protocol, from_port, to_port, cidr_ip, sg_id))
```

VISIBILITY BUILDS CONFIDENCE

I know exactly where we have issues.	We're catching issues in Dev.	We're Compliant in the CLOUD!!	Our controls match our policy.	I know the team is making the right moves.
				
SECOPS	DEVOPS	RISK & COMPLIANCE	CISO	CXO

EXAMPLE: CONTINUOUS INNOVATION



EXAMPLE: FINANCIAL INSTITUTION

- Rapidly deliver new industry apps in the cloud
- Eliminate need for developers to learn complex regulations
- Apps are secure when they are deployed, not fixed later

EXAMPLE: PREVENT DATA EXPOSURE

Ticketing App

Service Ticket Attachments

Sensitive Data

- Classify Data: PCI
- Check Exposure: Public
- Auto-remediate: Fix ACL

EXAMPLE: MAJOR MEDIA COMPANY

- Use S3 buckets for media file collection from partner networks
- Mix of web site content and media sharing in S3 between teams
- Legally liable for media exposure

REAL WORLD IMPACTS

Defense Contractor
Major Political Party

Amazon S3 **misconfigured**

60K files, 28GB of data, unencrypted passwords

1.1 TB of personal voter data including names, addresses

Major Financial Institution

Unpatched open source software with a **known vulnerability**

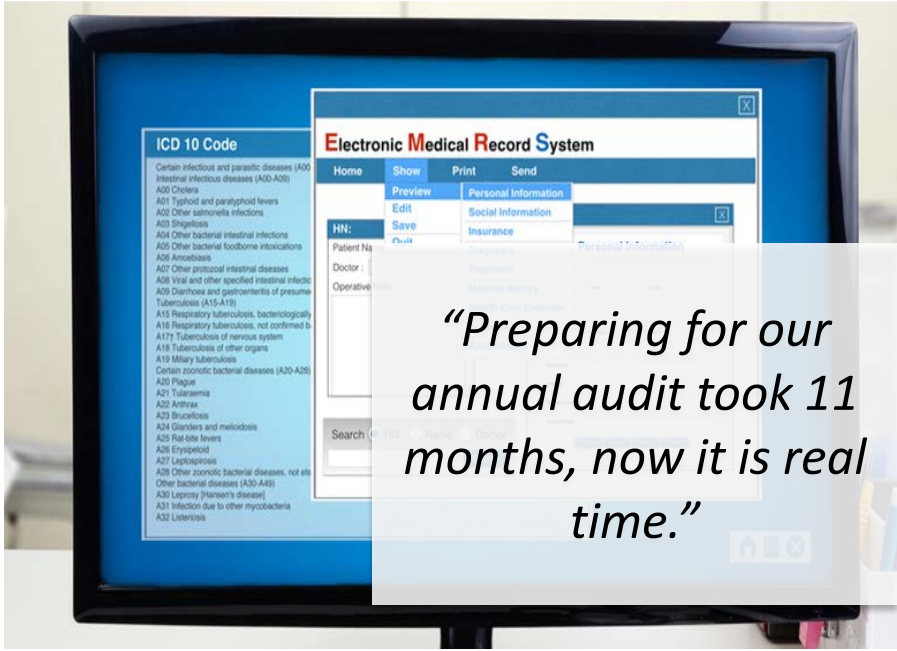
143 Million customers sensitive data exposed

EXAMPLE: COMPLIANCE VALIDATION AT SAAS COMPANY

- PCI, NIST 800-53 Compliance in AWS GovCloud
- Reporting and management takes only 1 person
- Ensures DevOps teams meet commitments to the business with every deployment

EXAMPLE: ELECTRONIC MEDICAL RECORDS PLATFORM

- Accelerate audit cycles – minimize disruption to business
- Build customer trust in online medical record transfers
- Mitigate vulnerabilities to sustain compliance



COMPLIANCE MATTERS NOW

PCI DSS:

4 Accounts

12 Testable Controls

2,813 control checks

X 2.5 minutes per

117.2 hours

NIST 800-53:

1 Account

35 Testable Controls

9,534 control checks

X 2.5 minutes per

397 hours or 10 weeks!

SECURITY IS A TEAM SPORT

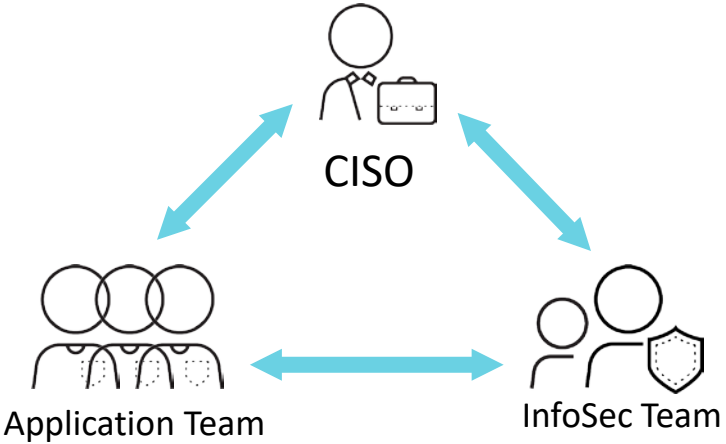
Fits into the organization-wide view of risk

Integrates with cloud development process

Automates prevention of complex threats

Enables teams to collaborate across roles

APPLY IT TODAY!



Bring key stakeholders together into one agile team