RSAConference2019

San Francisco | March 4 – 8 | Moscone Center

BETTER.

SESSION ID: LAB3-R02

Threat Hunting Across Thousands of Multicloud Workloads

Matt Chiodi

Chief Security Officer, Public Cloud
Palo Alto Networks
@mattchiodi

Gaurav Kumar

Chief Architect, Public Cloud
Palo Alto Networks
@gauravphoenix

#RSAC

Agenda

- Cloud vs. On-premise Security (10 min)
- Unit 42 Cloud Threat Research (5 min)
- Capture the Flag Challenges
  - Privilege Escalation Through IAM Instance Profile Role (30 min)
  - Instance Metadata API - Vulnerable Reverse Proxies (30 min)
  - Instance Metadata API - Malicious Docker Images (30 min)
- Wrap-up (5 min)

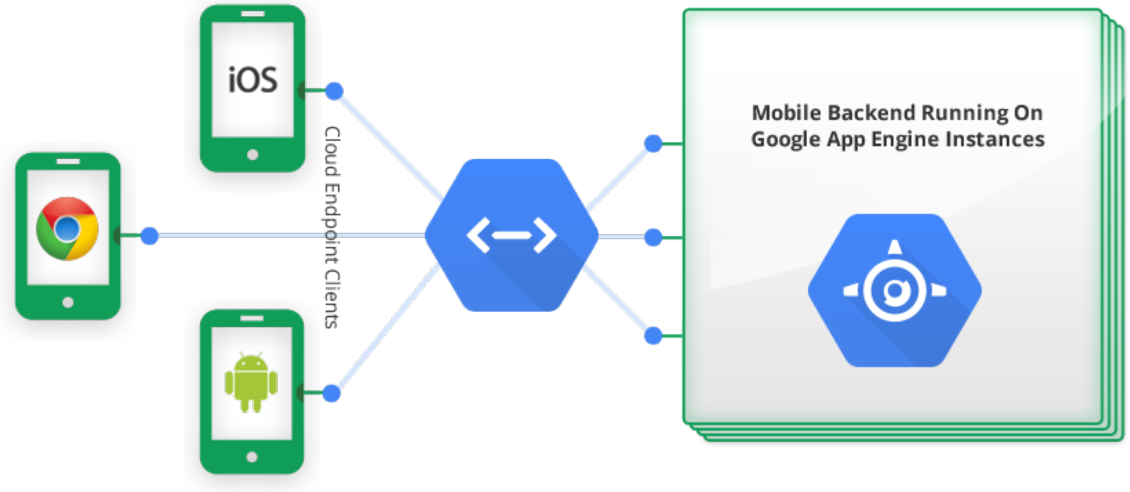
RSAConference2019

Cloud vs. On-Premise


"Security that exploits the programmatic nature of public cloud platforms via standards and automation." @mattchiodi

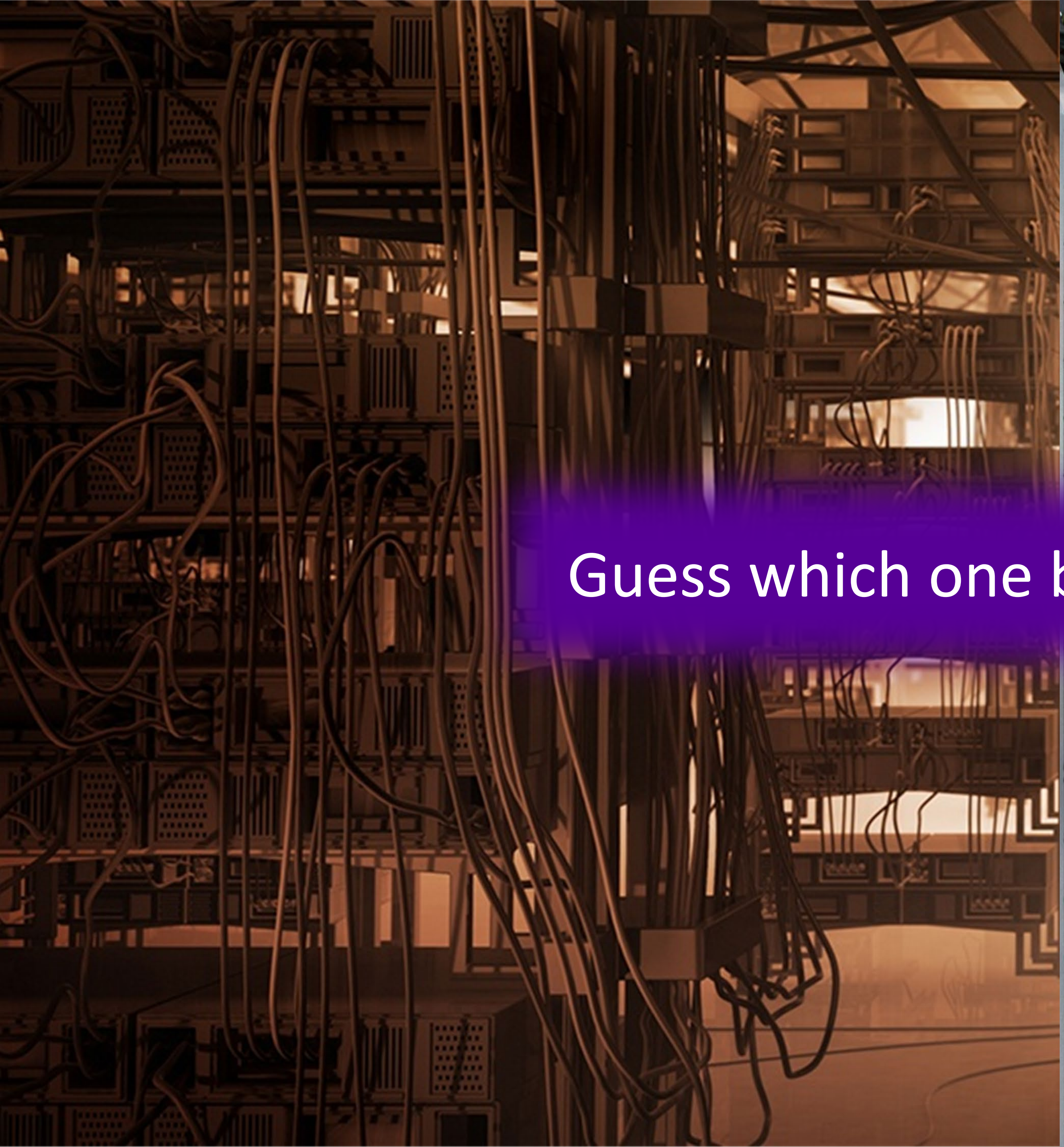
Programmatic: The Power of the API

- Asset inventory in real time...but
- Configuration in real time...but
- Near “complete” log visibility...but



Standards: The Precursor to Automation

- Promote interoperability with a multi-cloud strategy
- Enables an easier path to regulatory compliance e.g. HIPAA, GDPR, PCI DSS, etc.
- Makes everyone’s jobs easier (later)



Guess which one belongs to Google?

Automation: The Holy Grail

What's *Really* Different?

On-Premise	Public Cloud
- Organization responsible for security end to end	- Shared security responsibility with cloud provider
- Disconnected security tools; not typically driven by APIs	- Interconnected, API-driven security tools
- Static resources, perimeter-based security boundaries	- Dynamic resources, dynamic security boundaries
- Rarely automated	- Can be highly automated
- IT-driven	- Developer-driven

Seen This Before?

Organization

Responsible for security "in" the cloud

- Data Security
- Hosts & Containers
- Networks
- Users & Credentials
- Resource Configurations

Cloud Service Provider

Responsible for security "of" the cloud

- PaaS Core Functions
- Routers
- Switches
- Hubs
- Hypervisor
- Data Center

Common Public Cloud Security Pain Points

Decentralized Administration & Lack of Visibility

- No CMDB, real-time asset inventory or network topology diagrams exist for public cloud
- Large number of privileged users with little governance

Impact

- Increased likelihood of undetected misconfigurations
- Inability to quantify risk to management and board

Complexity of Compliance Management in the Cloud

- Hundreds of unique cloud services, with more added daily
- Proving compliance to auditors challenging in dynamic environments

Impact

- Stalled or delayed digital transformation initiatives
- Increased costs in achieving compliance

Inability to Rapidly Detect & Respond to Threats

- Traditional SIEMs do not have cloud context, and are unable to adapt to large data volumes and speed of change in public cloud

Impact

- Alert fatigue due to constant changes
- Extensive delays in investigating alerts with no context

RSAConference2019

unit42

unit42.paloaltonetworks.com

Cloud Threat Research

Account Compromises

29%

On average, **29%** of organizations experienced potential account compromises

Cryptojacking

11%

11% of organizations currently have cryptojacking activity in their environments

Promiscuous Network Policy

32%

46% of organizations accept traffic to Kubernetes pods from any source

Weak Identity & Access Mgmt.

23%

15% of organizations don't use IAM policies to control access to Kubernetes instances

RSAConference2019

Hunting Threats & Capturing Flags

The Challenges

- Privilege Escalation Through IAM Instance Profile Role
- Instance Metadata API - Vulnerable Reverse Proxies
- Instance Metadata API - Malicious Docker Images

Rules of Engagement

- Stay in our lab environment
- Whoever captures the flag first will win a “prize” (TBD)
- Whoever captures all the flags wins the “mega prize” (TBD)
- 30 minutes for each challenge

Privilege Escalation Through IAM Instance Profile Role

- Configure your AWS CLI to use provided credentials.
- The credentials do not have access to the s3 bucket but they do allow any operation on “EC2” service- including but not limited to listing of ec2 instances and their roles
- *Your mission, if you choose to accept it, is to access the s3 bucket.*

Instance Metadata API - Vulnerable Reverse Proxies

- You need to exploit a vulnerability in the reverse proxy (running on an ec2 instance) provided to you.
- The URL provided to you is a reverse proxy which fetches the content from the backend server specified in the “host” http header.
- *Your mission, if you choose to accept it, is to get IAM credentials from (of) the reverse proxy server.*

Instance Metadata API - Malicious Docker Images

- You are provided with a Jenkins URL. The job "buildDockerImage" takes a GitHub GIST URL which must point to a Dockerfile. The job, when run, builds a docker image.
- *Your mission, if you choose to accept it, is to steal AWS IAM credentials (of the Jenkins server) using the AWS IAM instance metadata API.*

RSAConference2019

The Wrap Up

Take Action!

- First 30 Days
  - Determine if instance metadata APIs are in use in your cloud environments
- Within 60 days
  - Follow principle of least privilege; utilize iptables to only allow root user to access
  - Review all 3rd party docker images in use; specifically ONBUILD commands
- Within 90 days
  - Apply security across build, deploy and runtime for containers
  - Identify vulnerable container images in registries, make sure only signed/scanned images deploy and watch runtime drift