RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

SESSION ID: SEM-M04

Cloud: Deployment specific attacks and remedies, containers, webapps, SaaS hosted services

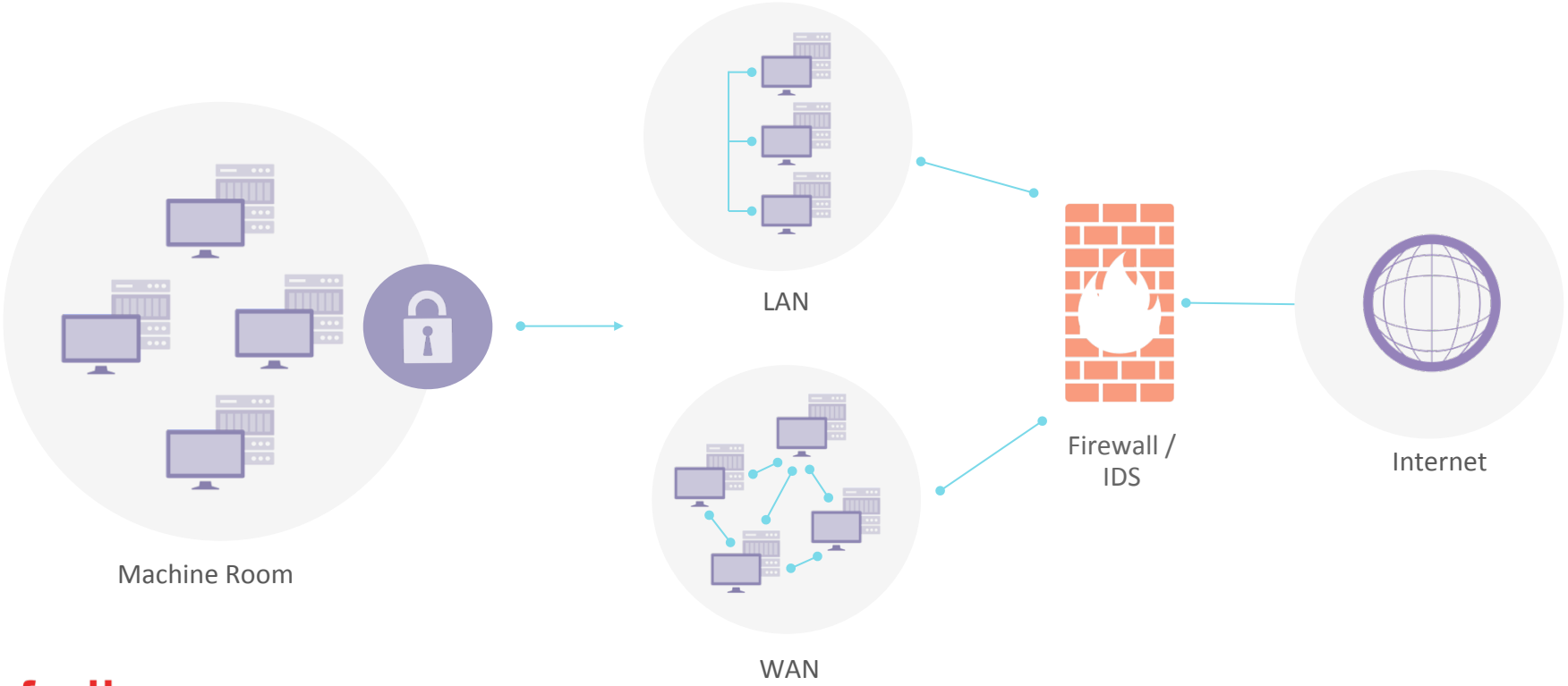
Dana Elizabeth Wolf

VP Product, Fastly
@dayowolf

Agenda

- Evolution of architecture
- Definitions of the major innovations in this space
- Threats that come along with these new technologies
  - Web apps
  - SaaS
  - Containers
- Quick wins to apply what you learned

In the beginning...



Then cloud happened

New challenges with new tech

Same security issues

1. Protect users
2. Protect data
3. Protect infrastructure

New architectural challenges

1. Users are mobile and identities are not natively managed in a central location.
2. Data is everywhere & not necessarily under your control.
3. Infrastructure isn't always yours & often shared by multiple customers.

It's easy to spin up new architecture quickly,
but hard to understand the security impact.

Definitions

Web app

- Programs accessed in a browser to perform tasks on the internet
- User has some degree of control
- Interactive

SaaS

- Software distributed as a service, available online.
- Inclusive of websites & web apps and also mobile & desktop applications

Containers

- Image of a modular package with a piece of software that includes everything needed to run it (code, runtime, system tools, system libraries, settings)

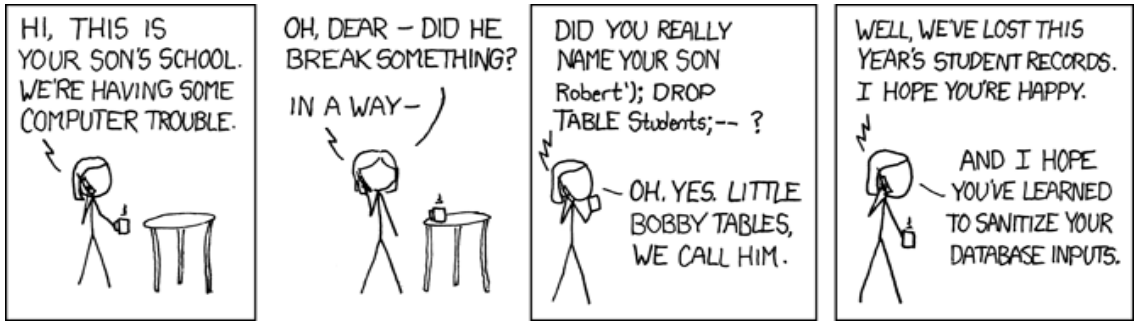
WEB APPLICATIONS

Web application security

OWASP Top 10 // 2013		OWASP Top 10 // 2017
1 Injection	→	1 Injection
2 Broken Authentication and Session Management	→	2 Broken Authentication
3 Cross-Site Scripting (XSS)	↘	3 Sensitive Data Exposure
4 Insecure Direct Object References (merged + 7)	U	4 XML External Entities (XXE) NEW
5 Security Misconfiguration	↘	5 Broken Access Control (merged)
6 Sensitive Data Exposure	↗	6 Security Misconfiguration
7 Missing Function Level Access Control (merged + 4)	U	7 Cross-Site Scripting (XSS)
8 Cross-Site Request Forgery (CSRF)	✖	8 Insecure Deserialization NEW (community)
9 Using Components with Known Vulnerabilities	→	9 Using Components with Known Vulnerabilities
10 Unvalidated Redirects and Forwards	✖	10 Insufficient Logging & Monitoring. NEW (community)

Weaksauce code: Injection (OWASP 1,3,7,9)

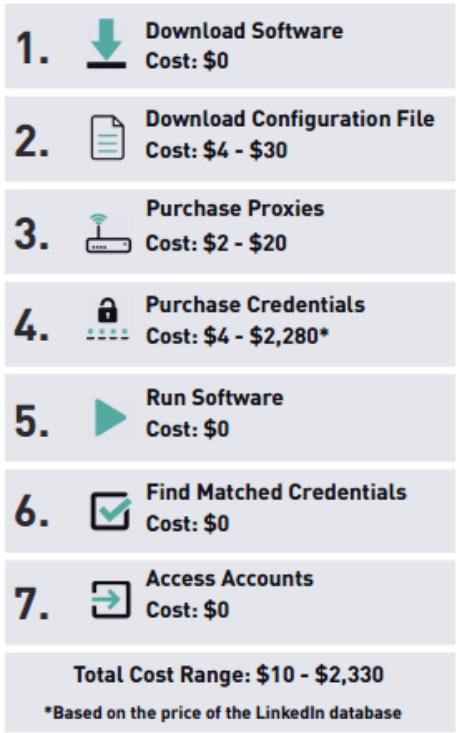
- Attackers send data to an app in a way that changes the meaning of the command to an interpreter.
- This was present in the latest Equifax, GoDaddy, and Wordpress breaches.
- “101 OR 1=1” instead of 101



Auth & Access Control: Broken Authentication (OWASP 2, 5)

- Weak credential management that allows user to act outside their intended permissions.
- Password123
- Username: admin, password: admin
- Criminals have written credential stuffing tools
- https://www.haveibeenpwned.com

Here's how easy it is to get stolen creds→



Config/Maintenance: Security Misconfiguration (OWASP 4, 6, 8, 10)

- Don’t use default admin accounts and passwords.
- “Here take my keys!”
- Sample applications & vulnerabilities
- List directories
- Detailed error messages with sensitive info → “this username and password combo is invalid”
- Default sharing permissions

Securing web apps

	Developers	Sec eng + testing	Leadership
Tools & processes	Static Application Security Testing (grammar check for developers)	Use a WAF and apply OWASP Top 10 in rules Automated testing of prod site: DAST (Dynamic application security testing) Pentesting - manual	Establish policies, training, and support for developers and project teams Integrate testing into existing processes Look for reporting across security tools
Approach	Follow the secure development lifecycle, design security from the start, and educate yourself in AppSec practices	Make testing compatible with the software development lifecycle (SDLC) Communicate security findings effectively.	Use a risk based portfolio approach Consider which security controls/tools fit with the needs of your organization Manage with metrics

SAAS/PAAS/IAAS

Cloud Threats: The Treacherous 12

2010	2013	2017	Top Threats
5	1	1	Data Breaches
N/A	N/A	2	Insufficient Identity, Credential and Access Management
2	4	3	Insecure Interfaces and APIs
N/A	N/A	4	System Vulnerabilities
6	3	5	Account Hijacking
3	6	6	Malicious Insiders
N/A	N/A	7	Advanced Persistent Threats
5	2	8	Data Loss
7	8	9	Insufficient Due Diligence
1	7	10	Abuse and Nefarious Use of cloud services
N/A	5	11	Denial of Service (DoS)
4	9	12	Shared technology vulnerabilities

Data Breach & Data Loss

Definitions:

- Breach = Unauthorized people get access to data
- Loss = Destruction, theft, data corruption. Data is lost forever

New Threat Vectors

- 3rd Party access to your data
- Data Loss is similar, but exacerbated
  - Secure Tunnel != Protection of Data
  - Losing encryption key
  - Offline backups

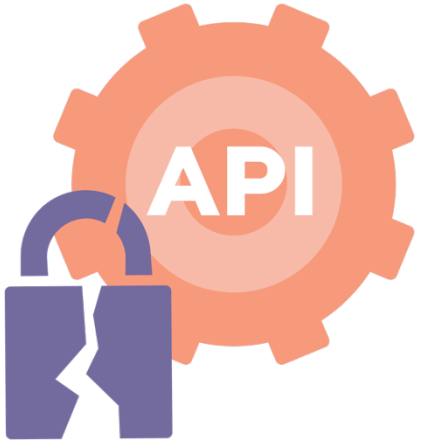
Insecure APIs

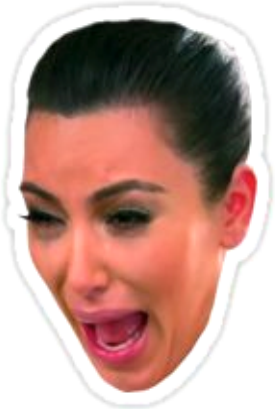
What is it about?

- APIs enables cross-cloud compatibility

What are API attacks?

- Kardashian Website Security Issues
- The Buffer attack – due to improper OAUTH code





Abuse and Nefarious use of Cloud Services

What is it about?

- Cloud services are nearly always accessible and enterprises rarely block them
- Attackers hide nefarious traffic in with legitimate traffic

How does it happen?

- Free trials and fraudulent account sign-ups expose cloud computing models
- Commonly used in DDoS, email spam, and phishing

Insufficient Due Diligence

What is it?

- Investigation into a CSP prior to signing a contract. Clarity on SLAs

Why does it matter?

- You are now more dependent on another provider for success of your business
- Added complexity of auditing multiple vendors' security
- Where cloud data resides, different laws apply

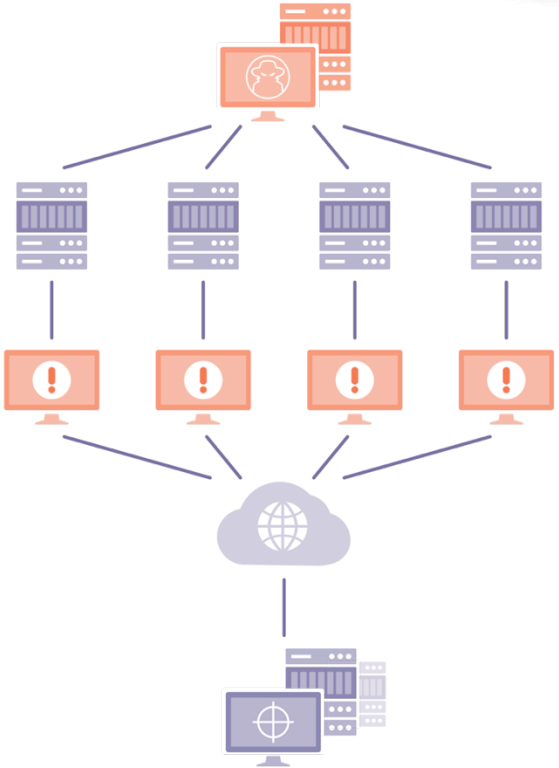
Denial of Service (DDoS)

What is it about?

- An attempt to make a machine or network resource unavailable to its intended users

How have attacks changed?

- Frequency: attacks per month on the rise
- Complexity
- Size: Largest attack in 2004 was 8 Gbps; Now upwards of 1.35 Tbps
- Collateral Damage



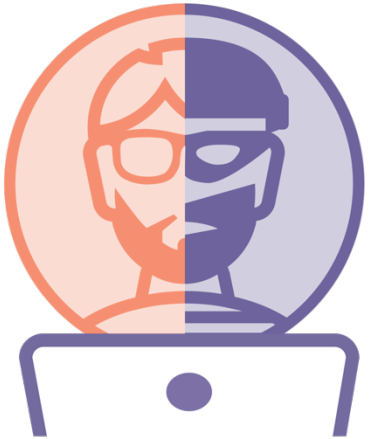
Shared Technology Vulnerabilities

What is it?

- Hardware used for common cloud services may not be hardened & misconfiguration is easily exploited

Why does it matter?

- Vulnerabilities in your software or SaaS supply chain become your problem
- A single vulnerability or misconfiguration can lead to a compromise across an entire provider's cloud



Getting a handle on cloud security

Visibility

You can't control what you can't see. Correlate across systems using log manager, SIEM, and behavioral analytics.

- Secure web gateways (SWG)
- CASB
- Endpoints (incl servers, hosts, mobile)
- Log log log

Data breach & data loss

Focus on reducing harm: For data breach situations, look at DLP and Encryption. For data loss, think backups.

- Use SSL for all traffic
- Invest in encryption, tokenization, key mgmt
- Understand your CSPs Disaster & Recovery Service

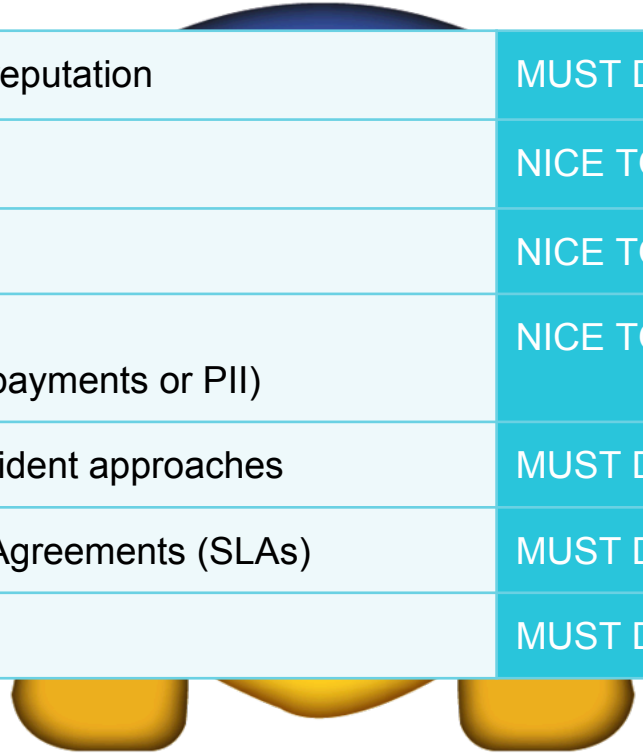
DDoS protection

Your infrastructure needs to withstand spikes in traffic.

- Use CDN to absorb traffic
- Use native DDoS protection in cloud storage services

Researching vendors

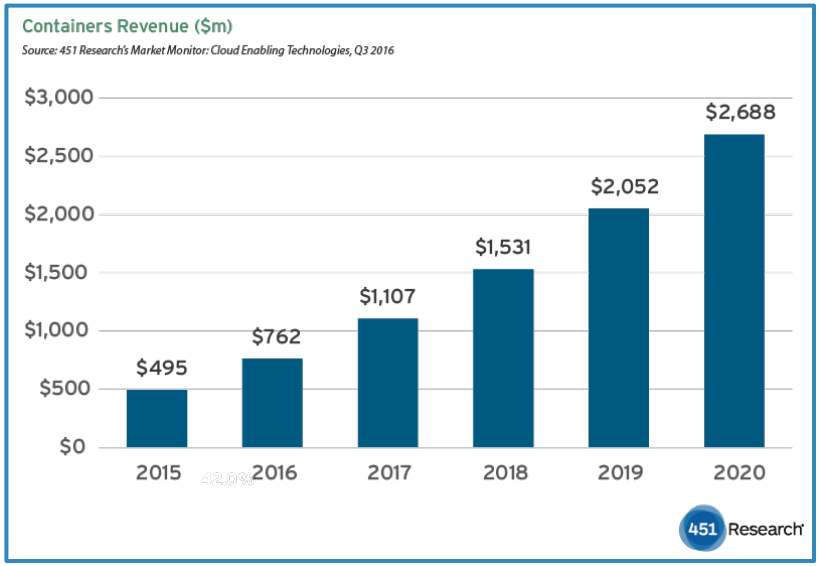
Check out CSP vendor's reputation	MUST DO
ISO27001	NICE TO HAVE
SOC2	NICE TO HAVE
PCI (if you accept any sort of payments or PII)	NICE TO HAVE
Bridge Maintenance & Incident approaches	MUST DO
Review all Service Level Agreements (SLAs)	MUST DO
Legal protection	MUST DO



CONTAINER

Container Threats Overview

- References:
  - NCC Group: *Understanding and Hardening Linux Containers*
  - Anthony Bettini: *Vulnerability Exploitation In Docker Container Environments*
- Threat Vectors:
  - The Linux Kernel
  - Container threats
  - Orchestration
  - Malicious and Vulnerable Images
  - Vendor specific threats

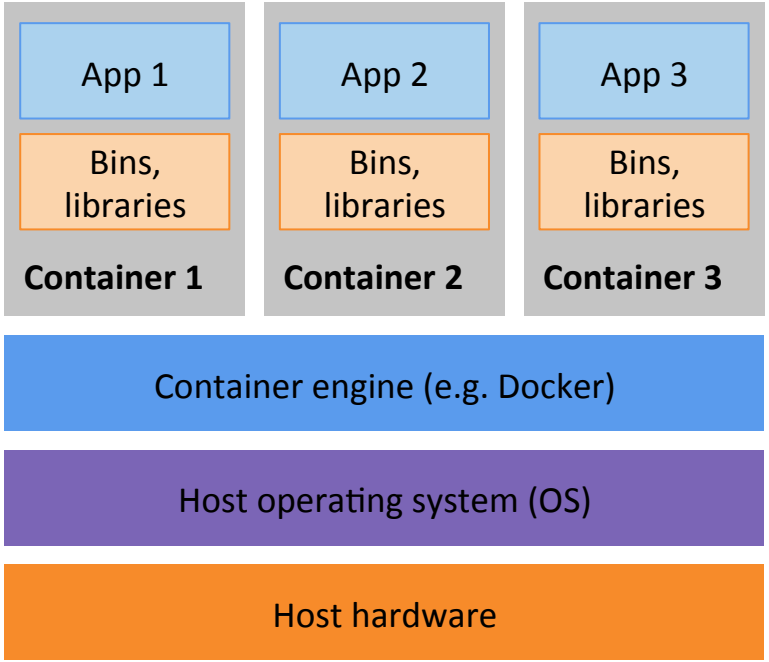


Vulnerabilities with Linux Kernel

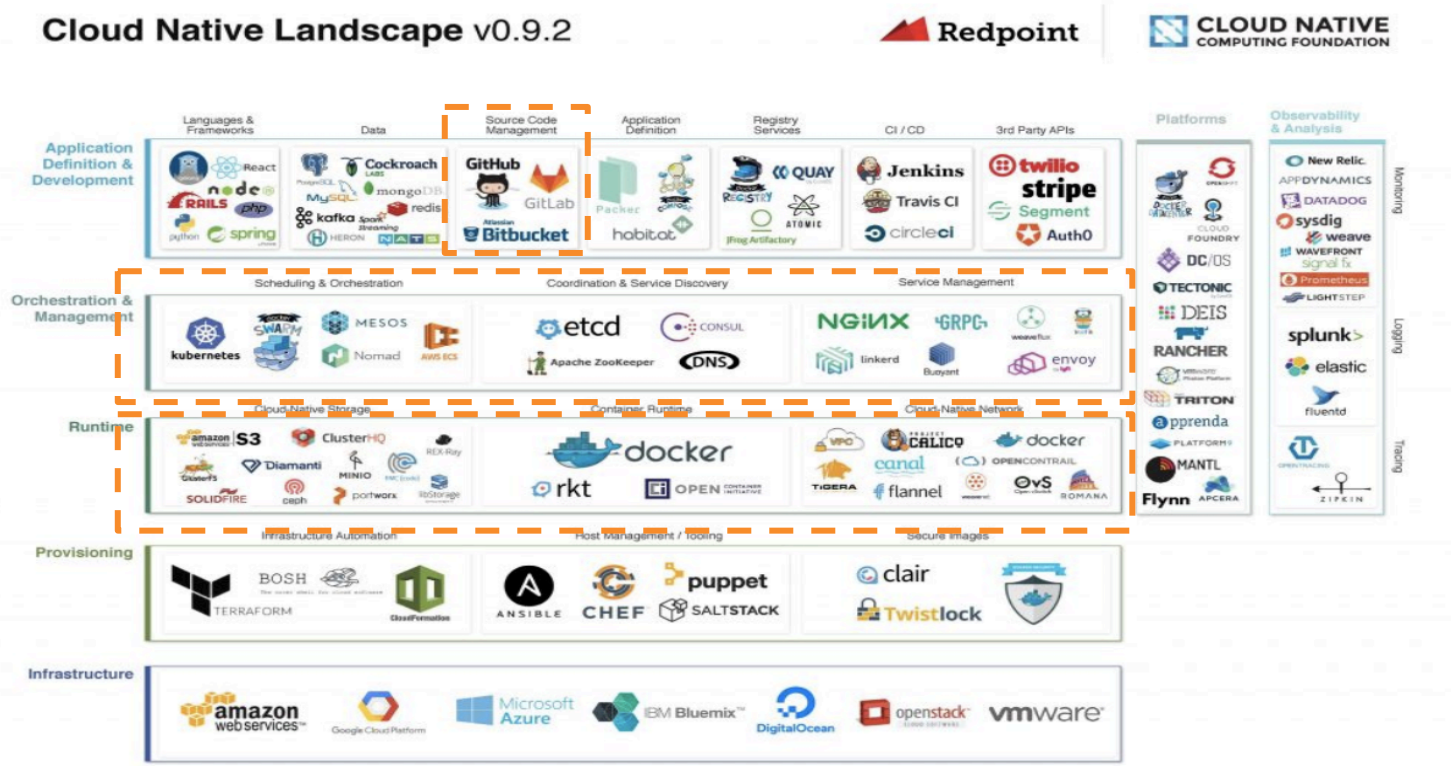
- Optimized for performance, not security
- A few things to note
  - Multiple containers will share a host OS and kernel
  - 2009 Pwnie award for “Lamest vendor response”

Types of container threats

- Escaping the container
- Cross-container attacks
- Inner container attacks
- Denial of service & resource consumption
- New code



Ecosystem


Cloud Native Landscape v0.9.2
Redpoint
CLOUD NATIVE COMPUTING FOUNDATION
Languages & Frameworks
Data
Source Code Management
Application Definition
Registry Services
CI / CD
3rd Party APIs
Platforms
Observability & Analysis
Application Definition & Development
React
node
RAILS
php
python
spring
Cockroach
MySQL
mongoDB
redis
kafka
GitHub
GitLab
Bitbucket
Packer
habitat
QUAY
Jenkins
Travis CI
circleci
twilio
stripe
Segment
Auth0
Scheduling & Orchestration
Coordination & Service Discovery
Service Management
Orchestration & Management
kubernetes
SWARM
MESOS
Nomad
AWS ECS
etcd
CONSUL
Apache ZooKeeper
DNS
NGINX
GRPC
linkerd
Buoyant
envoy
Cloud Native Storage
Container Runtime
Cloud Native Network
Runtime
amazon S3
ClusterHQ
Rex-Ray
Diamanti
MINIO
SOLIDFIRE
ceph
portworx
docker
rkt
OPEN
VPC
CALICO
docker
canal
OPENCONTRAIL
TIGERA
flannel
OvS
ROMANA
Infrastructure Automation
Host Management / Tooling
Secure Images
Provisioning
BOSH
TERRAFORM
CloudFormation
ANSIBLE
CHEF
puppet
SALTSTACK
clair
Twistlock
Infrastructure
amazon web services
Google Cloud Platform
Microsoft Azure
IBM Bluemix
DigitalOcean
openstack
vmware
CLOUD FOUNDRY
DC/OS
TECTONIC
DEIS
RANCHER
TRITON
apprenda
MANTL
Flynn
APCERA
New Relic.
APPDYNAMICS
DATADOG
sysdig
weave
WAVEFRONT
signal fx
Prometheus
LIGHTSTEP
splunk>
elastic
fluentd
ZIPKIN
Monitoring
Logging
Tracing

What you can do about container threats

- Hardening the host
- Reduce available attack surface, Limit network attack surface
- Update regularly
- Correlate with what's happening in across systems for more visibility and control

Bonus Cloud Threats for 2018

Meltdown

Spectre

APPLY

Apply What You Have Learned Today

After today, you should:

- Read up!
- Assess default configurations, controls & existing processes (patching, pen-testing, etc.)
- Get visible the visible
- Talk to people!

In the first three months you should:

- Risk assessment / Threat modeling – score yourself!
- Review existing contracts – score your vendors!
- Identify admin accounts and monitor them
- Identify which technologies would help extend visibility & control

Within six months you should:

- Rollout security hardening milestones for the company & begin execution
- Security education & secure coding
- Identify new processes to put in place to integrate CSP security with internal security workflow (cloud)

THANK YOU!