Application Security Essentials

Matthew Fisch
Founder & CEO, FortMesa

Application Security Essentials

Highlighted considerations:

“Code” Supply Chain	**Development Hygiene**	**Application Security**	**Platform Security**	**Security Architecture**
Can you depend on dependency security?	*Do you keep your source code clean and secure?*	*Do you control for threats unleashed against your software?*	*Do you have a plan to keep your application infrastructure secure?*	*Have you considered how these interrelate?* *Do you have an overall security strategy that covers all of these factors and others?*
We’ll touch on this.	We’ll touch on this.	**Recommended Reading:** OWASP Top Ten @ owasp.org ISACA CMMI @ cmmiinstitute.com	We’ll touch on this.	**Recommended Reading:** CIS CSC 20 @ cisecurity.org/controls/ NIST CSF @ nist.gov/cyberframework ISO 27000 @ iso.org

Cathedral vs Bazaar - Security Hygiene

Closed Source (Commercial)

- Good vs Bad Vendor Reputation
- Commercial Support
- Monolithic codebases
  - Overall quality

Open Source (FOSS)

- Well vs Poorly Managed Projects
- Community Stability / Backing
- Distributed codebases
  - Choosing components

- **How likely are you to find out about a vulnerability?**
- **How fast are you likely to get a fix?**
- **How easy is it to implement?**

Cyber Hygiene & Application Development

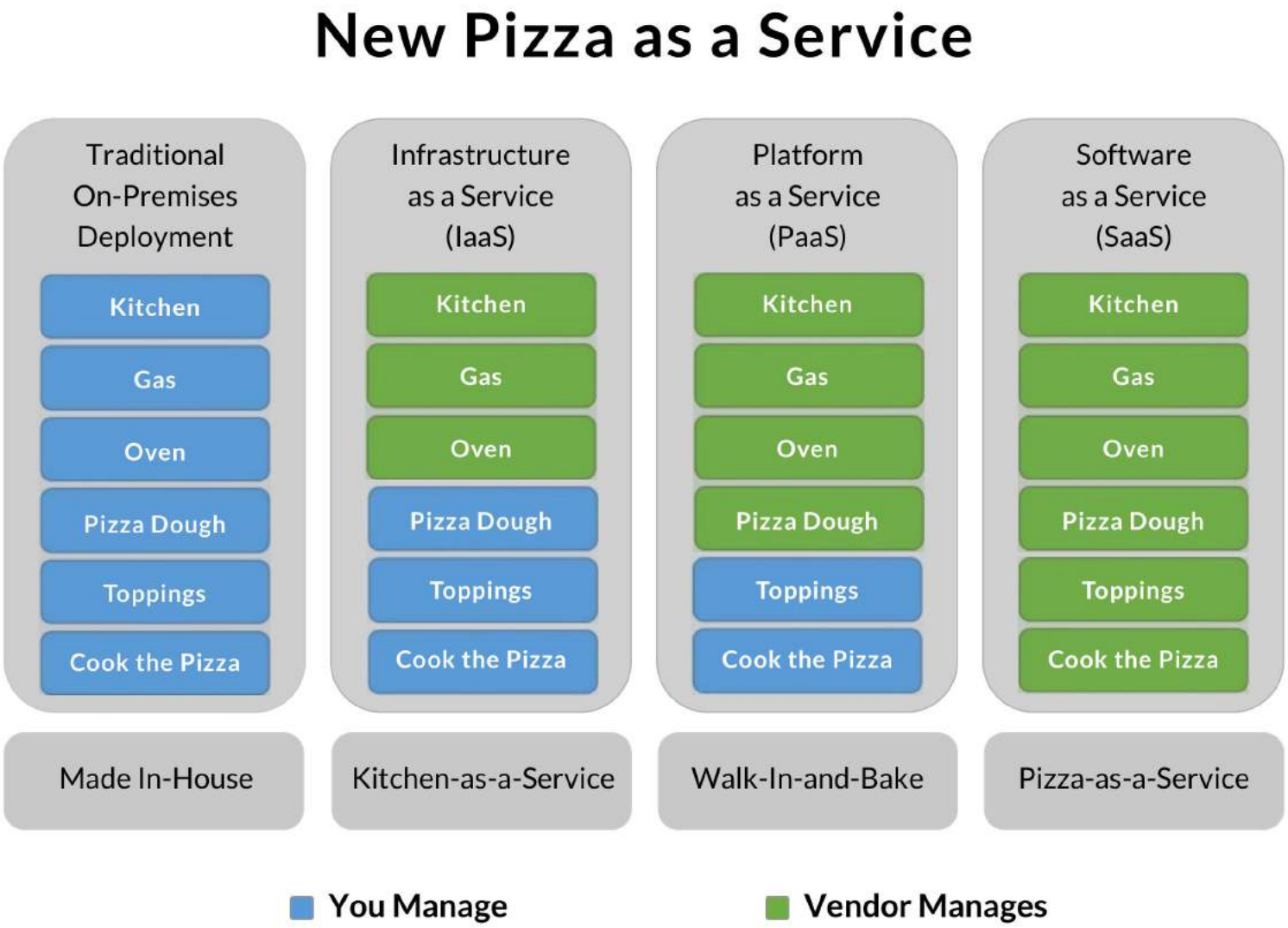
Supply Chain

- Are your sources from well known repos?
- Do your source dependencies support vulnerability audits?

```
$ npm audit fix
```

In Development

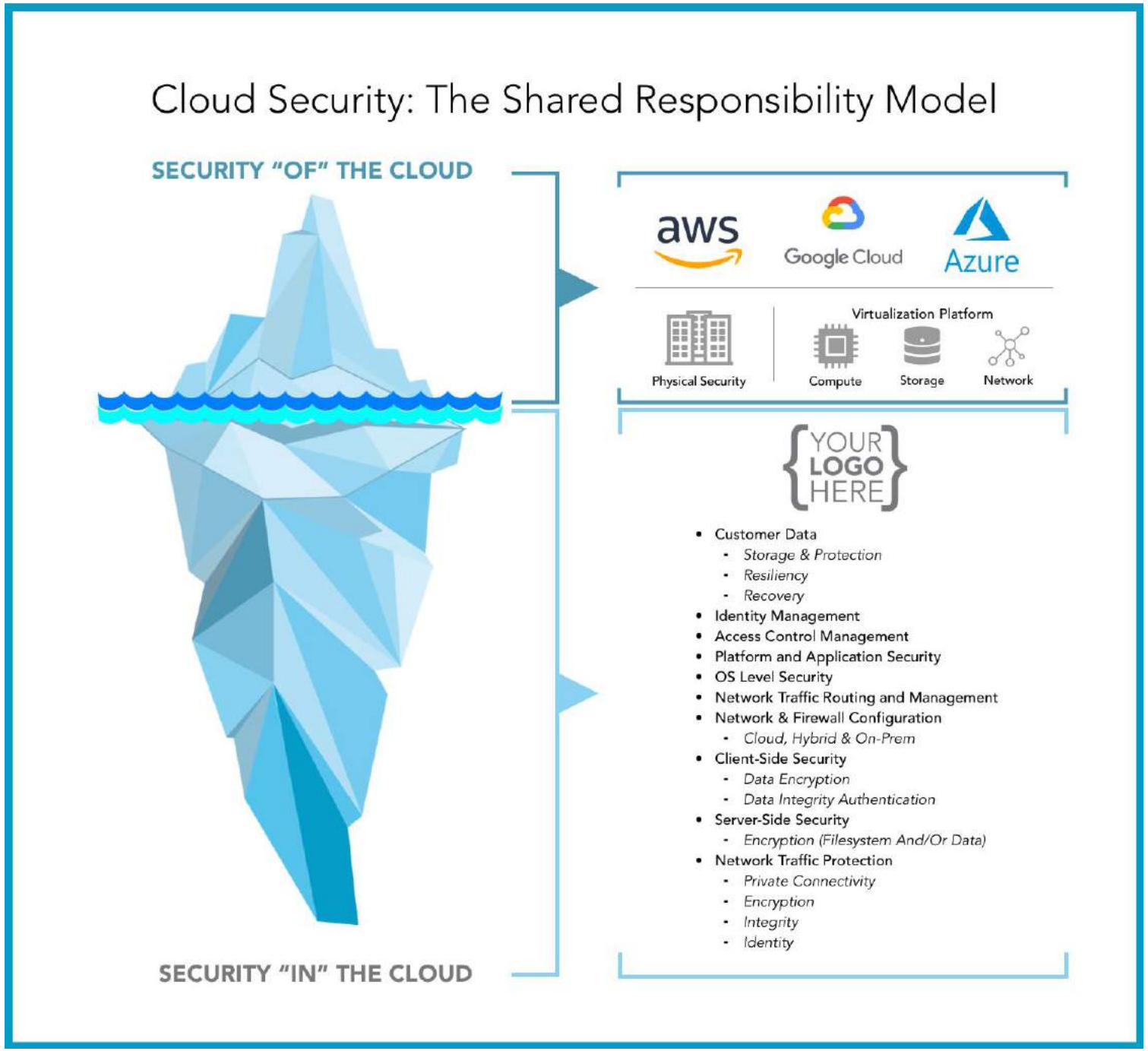
- Where do you store source code and how is it protected?
- Do you audit commits?
- Do you use dedicated development workstations?
- Do you ship builds from a personal workstation or a dedicated system?
- Are you using SAST/DAST and/or Other test automation?



XaaS Platform Security

- The cloud is not more or less secure than on-premise by default.
- aaS platforms shift the burden of due care and due diligence to an outside party.
- Do you trust them more or less than yourself?
- Is your time as a human best used keeping the fire going or creating something new?

HVTECHFEST 2019



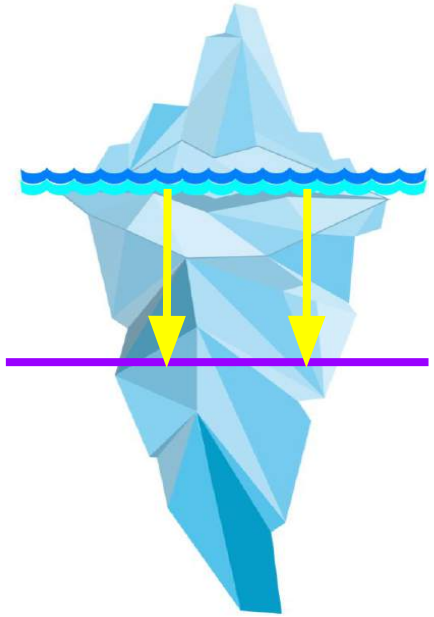
IaaS
Cloud Security

- **The cloud itself pretty much gold standard secure.**
  - Typically offers:
    - HITRUST / PCI
    - SOC 2 (SSAE 16)
    - ISO 27000
    - FedRAMP
- **Security inside the cloud …**
  - Did you do it?

Firebase App Engine

Engine Yard Pivotal

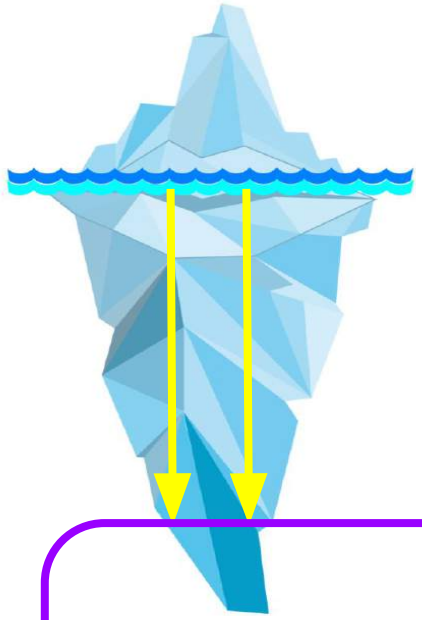
HEROKU



xPaaS Platform Security

- **Some PaaS operate higher or lower on the stack.**
- **Gartner:** ”As of 2019, the total PaaS market contains more than 360 vendors, offering more than 550 cloud platform services in 21 categories“

- **Infrastructure is done for you.**
  - Leverage someone else’s infrastructure engineers
  - Lower production maintenance overhead
- **You’re locked in:**
  - Platform maturity & cost.
  - Your security is only as good (and defined) as the platform’s security.
  - How much do you trust this company now and in the future?
  - You still need to devsec -- pay particular attention to the edges of the platform



SaaS Software Security

- **“Full security architecture” is an application buying criteria**

- **Access control is still super important**
  - Directories
  - MFA
- **Consider RBAC**

- **Infrastructure is done for you.**
  - Leverage someone else’s engineers
  - Lower production maintenance overhead
- **You’re locked in:**
  - Platform maturity & cost.
  - Your security is only as good (and defined) as the platform’s security.
  - How much do you trust this company now and in the future?
  - You still need to DevSec -- pay particular attention to the edges of the platform

Matthew Fisch, CISSP
Founder & CEO
FortMesa, Inc.

mfisch@fortmesa.com
phone: +1 518 444 4181
blog: blog.mfisch.com
web: fortmesa.com

FortMesa
Security culture on-demand.

Founder FortMesa
Stop cyber losses with on-demand security culture.

LinkedIn
Scan

Questions?

OpenHub
Innovation | Collaboration | Education

SUNY ORANGE

Mount Saint Mary College

ORANGE COUNTY NEW YORK 1 NOVEMBER 1683

OpenHub
Innovation | Collaboration | Education

SUNY ORANGE

Mount Saint Mary College

ORANGE COUNTY NEW YORK
1 NOVEMBER 1683