PROTECTING CONTAINERS FROM HOST-LEVEL ATTACKS

MODERATOR: Ben Jun
CEO, HVF Labs
@BenjaminJun

PANELISTS:
Ambuj Kumar
Co-founder and CEO
Fortanix Inc.
@ambuj0

David Lawrence
Security Lead
Docker
@endophage
What are Containers?

**VM**
- App A
- Bins/Libs
- Guest OS
- Hypervisor
- Infrastructure

**CONTAINER**
- App A
- Bins/Libs
- Guest OS
- Container Runtime
- Host OS
- Infrastructure
Missing gap in data protection

- Encrypt data at rest
  - Prevent disk theft and image theft

- Encrypt data in motion
  - Prevent snooping and unauthorized accesses

- Runtime / Data in use?
  - Vulnerable to misuse from attackers and insiders
Protect Data in Use: Runtime Encryption and Intel SGX

- Intel Software Guard Extensions (SGX) technology runs apps inside secure enclaves
- Runtime Encryption protects applications even when the infrastructure is compromised
Data in Use Protection for Apache Webserver
Notary Architecture
Docker Notary

Fortanix®
Runtime Encryption

docker

Intel SGX
Apply What You Have Learned Today

- Identify which containers you run today need runtime encryption
- Learn more about Intel SGX – visit the Intel booth at RSA
- Research cloud providers with SGX support – IBM Cloud, Microsoft Azure, and Equinix