PCI Security Standards Council®

2025 EUROPE COMMUNITY MEETING

2025
EUROPE
COMMUNITY
MEETING

Practical PCI DSS Compliance for Advanced Cloud Services and Architectures

A QSA's Perspective

PCI Security Standards Council

Gary Glover

CISSP, CISA, QSA

VP of Assessments

SecurityMetrics, Inc.

- 21 years Payment Card Industry
- Participate in SIG's, GEAR, etc.
- 10 years as a Software Developer
- 7 years as an Aerospace Engineer

securitymetrics®

PCI Security Standards Council®

Agenda

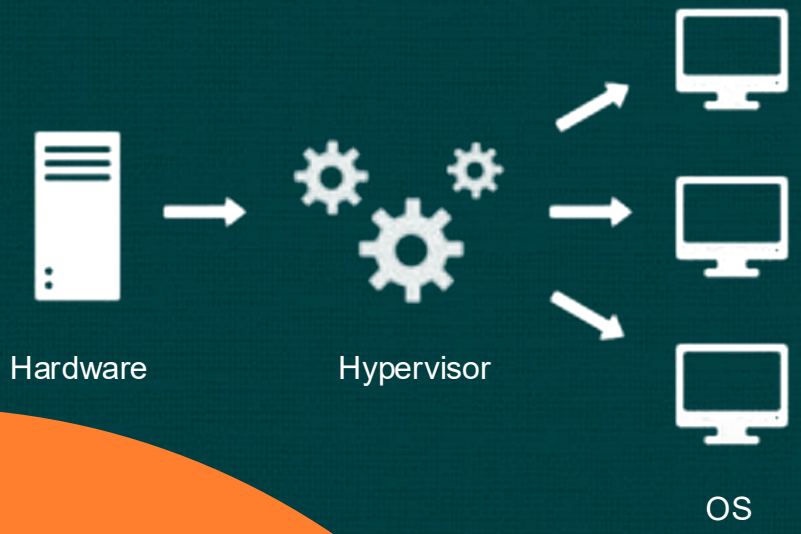
- Common Questions
- PCI DSS and Advanced Cloud
- Team up with QSA
- Assessing Advanced Cloud Solutions
- Hints for QSA’s
- Hints for Assessed Entities
- Take Aways

Common Questions

- Why does the PCI DSS not seem to cover the cloud technology I am using?
- Can our system be understood by QSA's?
- Is the technology we are using so advanced it can't be found compliant?
- Servers are becoming a thing of the past. Where do I apply PCI Requirements?

PCI Security Standards Council

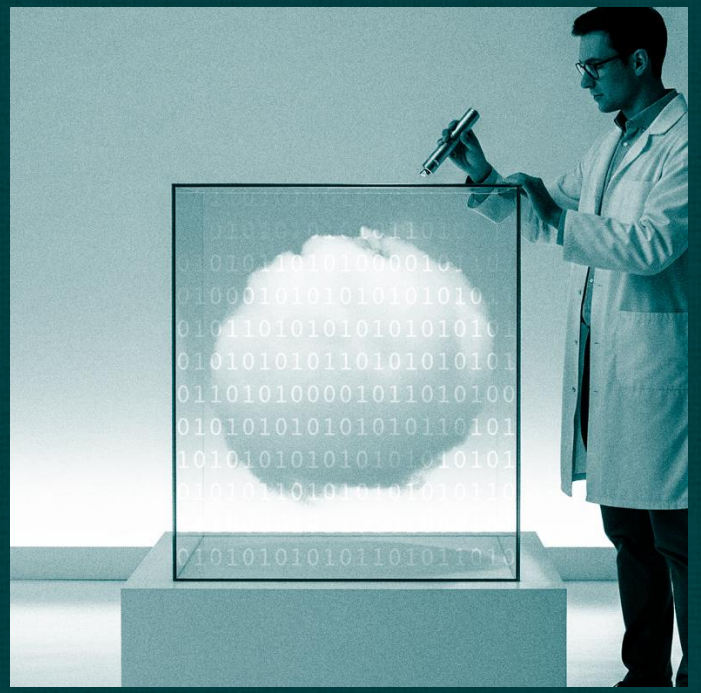
Traditional Cloud vs. Advanced Cloud Technology



- Traditional Cloud
  - VM's on Hypervisor(s), full OS images, virtual networking hardware, etc.
  - Mimics physical systems
- Advanced Cloud
  - Micro services (micro OS), Containers, Lambda functions, infrastructure as code, etc
  - Does not really mimic physical systems

PCI DSS and Advanced Cloud Tech

- Cloud solutions are rapidly evolving and increasingly used in Card Data Environments
- PCI DSS does not need to contain exact references to these new technologies
- Companies are frustrated when their cloud tools aren't directly addressed in PCI DSS, creating compliance uncertainty
- QSAs should focus on core PCI DSS principles to guide assessments and support organizations effectively



PCI Security Standards Council

Team Up With Your QSA on Advanced Cloud Tech

Apply Base Principals

- QSA communities' job is to work with clients to discuss core principals of PCI DSS requirements

Discuss Cloud Approach

- Provide detail on how you think a cloud technology will meet a PCI DSS req. be prepared to discuss

Focus Needed

- Be cautious about tech providing blanket coverage of for multiple PCI DSS requirements, confirm each

QSAs Can Learn

- QSAs can’t know everything, that is OK, we can all learn, pre-existing knowledge is not always necessary

Does it Measure Up?

- QSA and Client review requirement wording, objective, testing proc. to see if tech satisfies req.

Communicate

- Open communication between QSA and client is critical, keep open mind, work together

PCI Security Standards Council

Cloud Technology and Testing Procedures

- PCI DSS testing procedures may not match cloud tech exactly
- Don’t try to force traditional tools in all cloud situations
  - FIM, AV scanning, etc.
- Find where in the technology chain the requirement is met, focus on securing the environment
  - Example: FIM installed on a container may not make sense

Common Cloud Technologies Seen in Assessments

- Networking
  - Security Groups (AWS and Azure), Network ACLs, GCP VPC firewall rules, Load Balancers, WAF, Cloud IDPS services, Network monitoring services, etc.
- Containerization
  - Google Cloud Run, AWS EC2 & Fargate, Azure Container Instances, Azure Kubernetes Service, etc.
- Compute Functions
  - AWS Lambda, Azure Functions, Google Cloud Functions
- Infrastructure as Code (IaC)
- Storage (S3, Azure Blob, etc)
  - Various file encryption technologies to understand

PCI Security Standards Council

PCI DSS Requirements Most Discussed in Advanced Cloud Architectures

Section 1 – NSC
- Cloud equivalents

Section 2 – Standards
- Cloud hardening

Section 3 – Encryption
- Similar encrypt; key management systems

Section 4 – Transmission
- No real issues

Section 5 – Malware
- Non-Traditional Methods

Section 6 – Secure Dev
- No real issues

Section 7 – Authentication
- May not be OS based

Section 8 – Passwords
- No real issues

Section 9 – Physical
- SP responsibility

Section 10 – Logging
- No real Issues

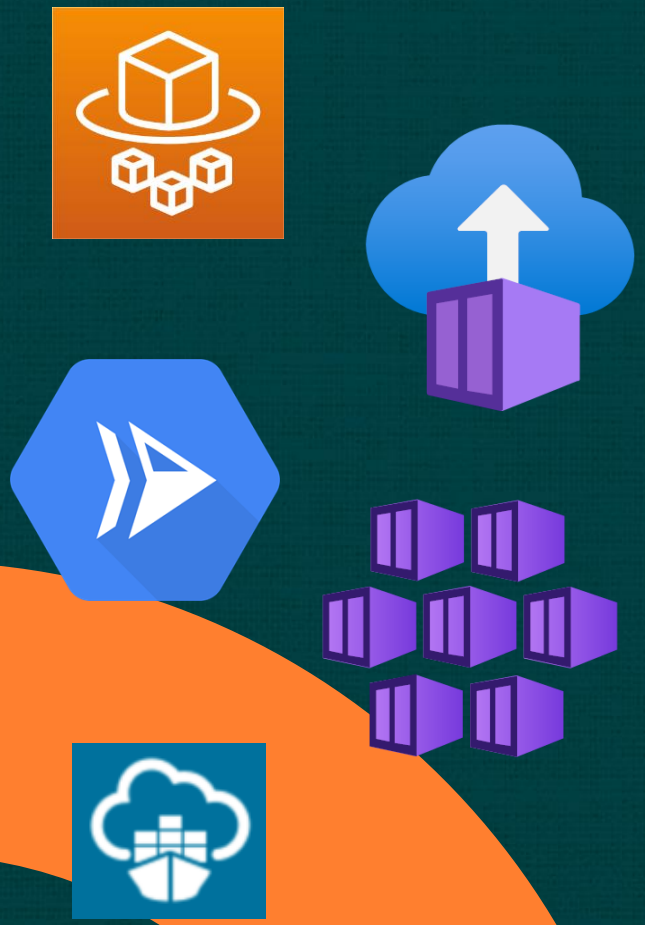
Section 11 – Test Systems
- FIM different, Internal VA scans and Pen Testing issues

Section 12 – Sec Policy
- Responsibility Matrix important

PCI Security Standards Council

Assessment Examples

- Always review objective of the requirement
- File Integrity Monitoring (Change Detection Mechanism)
  - FIM agent on container can be too much, look upstream to repository, etc.
  - Serverless functions, focus on changes to function code itself
- Malware Protection
  - Similar to FIM, look upstream, understand life of container
  - Serverless functions this becomes N/A
- Internal Pen Testing
  - Creating separate VPC for IPT is not ”real”, attack as low privilege cloud user role more realistic
- Infrastructure as Code (IaC)
  - Far upstream, TPSP monitoring changes/malware, spend time on IaC code repository



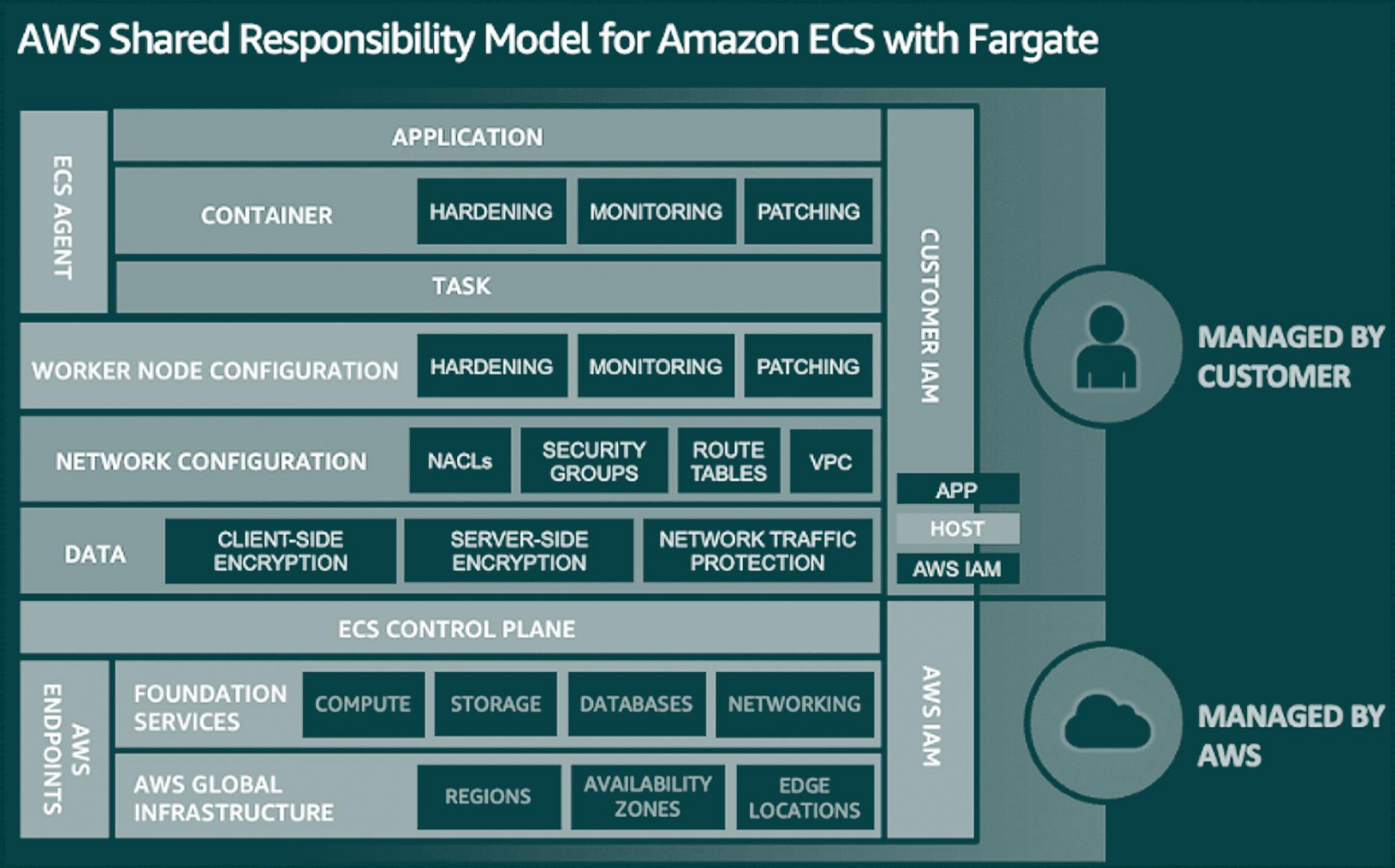
“Turnkey” Cloud Solutions

Serverless Container Compute Engines - Run containers without managing servers or clusters

- AWS Fargate
- Azure Container Instances
- Azure Kubernetes Service+Virtual Nodes
- Google Cloud Run, GKE Autopilot
- IBM Code Engine
- Oracle Cloud Container Instances
- Etc.

PCI Security Standards Council

AWS Fargate Shared Responsibilities



* “Security considerations for running containers on amazon ECS”, Nov 2023

PCI Security Standards Council

Hints for QSAs

- Don’t blindly apply “the old way” to new cloud environments
- Don’t get stuck on the words in the testing procedure
- Don’t overuse compensating controls, look “upstream” for controls
- Protect admin interfaces
- Focus on where unauthorized change can occur

Hints for the Assessed Entity

- Its OK PCI DSS does not use exact cloud wording
- Communicate with QSA, don't just assume they won't understand your advanced systems
- Don't dismiss QSA for not having exact cloud experience, let them research, QSA community is pretty smart generally
- Read PCI DSS, look for objectives, anticipate QSA questions
- Locate all the responsibility summaries from cloud providers
- Locate AOCs for cloud services you are using

Take Aways

PCI DSS strives to be technology neutral

PCI DSS is focused on security controls

Apply the objective and intent of the PCI DSS requirement to new technologies being used as security controls

Move your thinking “upstream” into advanced cloud technologies and find where compliance to a PCI DSS requirement happens

Questions?

Come see me at our booth or,
gglover@securitymetrics.com

PCI Security Standards Council