Cloud Security

Five Phases of Cloud Security
Our journey led us here

With more than a decade having passed cloud continues to be defined differently depending on perspective. Identifying effective cloud security is dependent on how your organization defines cloud and the operational model chosen to build and manage your environment (i.e. CI/CD, lift-and-shift, IaaS, PaaS, SaaS). Today, we will cover the following topics:

- How cloud customers have approached cloud security and some of the challenges they have encountered,
- Cloud computing is an operational model with patterns. We’ll talk about observations that developed the patterns presented today, and
- As more cloud customers are adopting multi-cloud solutions, how a holistic approach will set the foundation for future success.
About Me

- 20+ years in IT and security career spanning multiple disciplines
  
  application development and security, web development, compliance, middleware administration, SMB hosting, network security, SOA to microservices to PaaS

- CI/CD experience began in the data center in the early 2000’s, before “cloud”

- The experience from multiple disciplines led to building and deploying to AWS since 2007

- I have designed and built my own solutions since the early 2000’s, out of necessity

- Cloud Security Practice Director at GuidePoint Security, a pure-play cybersecurity solutions provider

Jonathan Villa
Practice Director, Cloud Security
jonathan.villa@guidepointsecurity.com
linkedin.com/in/jonathanvilla
“Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.“ (NIST 800-145)
MANY TYPES OF CLOUD CUSTOMERS

The journeymen along the cloud adoption path

Existing Ventures Corporation
Tactical implementation of cloud services
Compute
Storage

Smart Decisions Corporation
Strategic decision to adopt cloud
Big data solutions
Existing information security experience

Cautious Decisions Corporation
Tactical + Strategic
Vetted information security program
Security checklist

Solutions Everywhere Corporation
Using all PaaS services
Serverless application
NOTHING NEW UNDER THE SUN

Clouds are unique, so which pattern?

**Crawl, Walk, Run**
- Experience
- Proven
- Sounds Simple

**Denial, Forced, Acceptance**
- Cloud is a fad
- We have a new CIO
- Look at what we’ve built in the cloud

**CSP Patterns**
- AWS Strategy – The 6 R’s
- Rehost
- Replatforming
- Repurchasing
- Refactoring
- Retire
- Retain

- Azure – Cloud Adoption Framework
- Strategy
- Plan
- Ready
- Govern
- Manage
- Organize
First conversations focused on tactical solutions

- **WHAT IS THE NETWORK TOPOLOGY**
- **WHAT ARE THE SERVER HARDENING STANDARDS**
- **WHAT’S THE BEST WAY TO MANAGE DISK ENCRYPTION**
- **HOW DO WE MANAGE LOGS, ALERTING, & MONITORING**
TACTICAL APPROACH

First conversations focused on tactical solutions

DATABASES

WHAT IS THE NETWORK TOPOLOGY

WHAT'S OUR STRATEGY FOR DISASTER RECOVERY

WHAT'S THE BEST WAY TO MANAGE DATA ENCRYPTION

HOW DO WE MANAGE LOGS, ALERTING, & MONITORING
NEW BUT OLD PROBLEMS

Security considerations overlooked in the cloud

Unknowns

- Complicated Authorization
- Internet Accessible Storage
- Managing Exponential Inventory
- Responsible Cloud Spend
NOTHING NEW UNDER THE SUN

Clouds are unique, so which pattern?

LOGGING
- What do we log?
- Where do we store our logs?
- Do we encrypt the logs?
- How do we interpret our logs?

ENCRYPTION
- Do we use cloud native or a third-party key management solution?
- Who and what systems have access to data encryption keys and secrets?

AUTHORIZATION
Define
- Service
- Action
- Resource
- Condition
For
- 100’s of services
- 1000’s of actions
- Countless Resources
- Many conditional options

{ "Version": "2012-10-17",
  "Statement": [
    { "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Resource": "*" }
  ] }
Governance

Define the standards and direction forward

Project Mgmt.

Set the pace and staying the course
Building a strong foundation

1 FOUNDATION

Have you identified a current posture and baseline?

[AWS] How will root accounts be managed?

How will you address exposure and threats from new cloud services?

Which compliance requirements impact your business?

A “we run everything” tech stack is fine, but how does that impact standardization, efficiency, and agility?

Are you ok with managing multiple authentication mechanisms, separately?

Is your team adequately trained to adopt cloud computing?
As secure as your network is, a compromised privileged cloud identity will supersede any network security enforcement.

Identity management must be an early consideration, especially how to monitor and right fit your entitlements.

Network topologies have become easier. Take your pick, but ensure you have egress visibility.

Key management in the cloud can be trusted. A proper implementation can be secure, efficient, and extremely cost efficient.

However, understand that the cloud providers approach encryption different: data encryption, secrets, certificates.

Enforce encryption and data access using the same methods used to build business solutions.
You’re going to need a logging platform that helps you understand cloud events in addition to other events?

You will need to log cloud API activity, network traffic, infrastructure changes.

Automate your Change Advisory Board, all cloud resources and changes to them are logged and can be prevented or rolled back.

Most importantly, understand what to look for:

- Excessive denied API requests
- Anomalies in cloud API usage, even with successful least privilege policies
- Change in baselines, i.e. increased compute capacity or network ingress/egress traffic
- Understand what NOT to look at, i.e. rabbit holes
Compute instances are following configuration management, golden AMIs processes, hardened, roles/service principals only when needed

Serverless architectures are flexible but there is now visibility and continuous monitoring for improvements to access controls

You’ve deployed acceptable web application protection based on your PaaS architecture

You’re better prepared to accept the adoption of new cloud services

While public cloud service providers are different, you’re in a better situation to tackle the common denominators.

With cloud being a vast landscape of services, you’re in a good spot to align with other frameworks, e.g. the GuidePoint CSAF.
1 Foundation

- External Connectivity
- Organization Management
- GPS Security Controls

Cloud Security Controls

- Discovery & Health Check
- Root Requirements
- Service Control Policies
- Geographical Boundaries
- Financial Responsibility
- Compliance Requirements

2 Perimeter

- IAM
- Network Security
- External Connectivity

3 Data Protection

- Key Management
- Reporting
- Secrets

4 Visibility

- Monitoring
- Config
- Logs

5 Cloud Solutions

- Virtual Servers
- Databases
- IoT
- Containers
- Data Warehouse
- Mobile
- API Gateway
- Blob Storage
- CDN
1 FOUNDATION

EXTERNAL CONNECTIVITY
AZURE DEVOPS
IDENTITY GOVERNANCE
GPS SECURITY CONTROLS

DISCOVERY & HEALTH CHECK
ROOT REQUIREMENTS
SERVICE CONTROL POLICIES
GEOGRAPHICAL BOUNDARIES
FINANCIAL RESPONSIBILITY
COMPLIANCE REQUIREMENTS

CLOUD SERVICE ARCHITECTURE
THIRD-PARTY INTEGRATIONS
TECHNOLOGY STACK(S)
DEPLOYMENT METHODOLOGY
CLOUD SECURITY METHODOLOGY
DEFINE PROJECT MILESTONES

CLOUD SECURITY CONTROLS

2 PERIMETER

IAM
NETWORK SECURITY
EXTERNAL CONNECTIVITY

3 DATA PROTECTION

KEY VAULT
AZURE INFORMATION PROTECTION
CONDITIONAL ACCESS

4 VISIBILITY

ALERTS
SECURITY CENTER
ACTIVITY LOG
NETWORK WATCHER

5 CLOUD SOLUTIONS

VIRTUAL MACHINE
SQL SERVER
COSMOS DB
AZURE RESOURCE MANAGER
AZURE IoT
AKS
LOGIC APPS
AZURE INTUNE
AZURE API MANAGEMENT
BLOB STORAGE
MACHINE LEARNING
How does this apply to SaaS?

- Application and Data Security
- Identity and Access Management
- Compliance and Governance
- 3rd Party Tools and Add-Ons
- Device Security
- Foundation
- Perimeter Security & Incident Response
- Data Protection
- Visibility
- Cloud Solutions
<table>
<thead>
<tr>
<th>Foundation</th>
<th>Perimeter</th>
<th>Data Protection</th>
<th>Visibility</th>
<th>Cloud Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Establish a Cloud Steering Committee for oversight</td>
<td>- Define and implement RACI model based on current roles and future cloud roadmap</td>
<td>- Follow through on encryption requirements, act on them</td>
<td>- Implement known pattern of CloudTrail, VPC Flow Logs, Config, Guard Duty, Activity Logs, Security Center</td>
<td>- Build and implement IaC templates to standardize deployment of cloud resources</td>
</tr>
<tr>
<td>- Identify compliance requirements</td>
<td>- Update permissions based on actual activity in the cloud</td>
<td>- Work with developers to incorporate secrets management using native cloud services</td>
<td>- Consolidate your logs, somewhere.</td>
<td>- Use a “golden image” process and alert non-approved images are being used</td>
</tr>
<tr>
<td>- Define a cloud baseline and monitor it</td>
<td>- Ensure egress visibility is in place for awareness of what is leaving your cloud</td>
<td>- Don’t shy away from cloud native data protection services</td>
<td>- Identify what to alert, who should respond, and how to remediate cloud security events</td>
<td>- Ensure new cloud solutions have been approved by or are visible to the Cloud Steering Committee</td>
</tr>
<tr>
<td>- Identify account owners [AWS]</td>
<td>- Monitor and alert on deviations from your baseline, e.g. security groups, routes, gateways</td>
<td>- Monitor and alert on deviations from your baseline, e.g. volumes/buckets not encrypted</td>
<td>- Monitor and alert on deviations from your baseline, e.g. anomalies, failed API calls</td>
<td>-</td>
</tr>
<tr>
<td>- Provide cloud adoption training and cloud security training</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Define spend thresholds and alerts</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Cloud environments are diverse but security leaders have the foundation, some just need a blueprint.

There are historical challenges and new challenges.

Look down the path, is multi-cloud in your future?

Establish project management patterns for cloud computing.
Thank You

Jonathan Villa | Practice Director, Cloud Security