WELCOME TO

Cloud Security Posture Management

Mike Small
Senior Analyst | KuppingerCole
Digital Transformation
Through the use of cloud services
Digital Transformation
Brings new risks that must be managed

IT as a Service

**Agile**
Enables rapid Business-Led Change
but creates volatile services, workloads and resources.

**Flexible**
DevOps approach is flexible to business needs and customer feedback
but creates new risks.

**Responsive**
Just in Time Resources - Servers, Storage and Services on demand
but create new management challenges.
Three Major Concerns

That must be managed

1. **Compliance Failure**
   Fined $80M for hack that exposed 100 Million accounts

2. **Data Breaches**
   Fined £20m by UK (ICO) for a data breach affecting 400,000 customers.

3. **Business Continuity**
   REvil set the price of a universal decryptor at $70 million

---

### Biggest security challenges in multi-cloud environments

- Poor cloud architecture design and lack of network hygiene: 15.0%
- No control over privileged accounts with access to the cloud: 36.7%
- Credentials, secrets or data left unprotected in the cloud: 48.3%

Source: KuppingerCole Research
Challenge Infrastructure as Code
Capital One Data Breach 2019

1. Misconfigured WAF
   Relayed requests to a key back-end resource.

2. Excessive privileges
   The VM was assigned excessive privileges.

3. Used to Access S3
   To list and read the files and buckets even when encrypted.

4. $80M Fine
   OCC fined and required risk management changes.

10. After receiving this information, Capital One examined the GitHub file, which was timestamped April 21, 2019 (the “April 21 File”). Capital One determined that the April 21 File contained the IP address for a specific server. A firewall misconfiguration permitted commands to reach and be executed by that server, which enabled access to folders or buckets of data in Capital One’s storage space at the Cloud Computing Company.

11. Capital One determined that the April 21 File contained code for three commands, as well as a list of more than 700 folders or buckets of data.
   - Capital One determined that the first command, when executed, obtained security credentials for an account known as *****-WAF-Role that, in turn, enabled access to certain of Capital One’s folders at the Cloud Computing Company.
   - Capital One determined that the second command (the “List Buckets Command”), when executed, used the *****-WAF-Role account to list the names of folders or buckets of data in Capital One’s storage space at the Cloud Computing Company.

Capital One Indictment US District Court Seattle
Challenges

From the multi-cloud hybrid IT service delivery
Challenges in the Hybrid Multi-Cloud
Engineering Secure and Compliant Service Integration

Non-Cloud

- **New Silos**
  Apps are siloed in different clouds.

- **Privacy Enabled Data Security**
  Secure and private data sharing

- **Inconsistent tools and capabilities**
  For each cloud and on premises components lead to an ad hoc approach.

- **Ad Hoc Service Governance**
  Not cost effective and fails to meet business needs

Multi Cloud
Multi-Cloud Hybrid Today
What vendors offer and what customers are using

Non-Cloud

- Private Cloud Tools
  - VMware
  - OpenStack
  - Cloud in box
  - Terraform
  - Hardware as a Service

- Public Cloud Tools
  - Vendor Templates
  - Vendor Monitoring
  - Vendor Compliance

- Container Tools
  - Kubernetes
  - Anthos
  - Docker
  - Red Hat OpenShift

- Legacy Tools
  - Vulnerability Mgt.
  - Identity Mgt.
  - Network Mgt.

- New Tools
  - CSPM
  - CWPP
  - CNAPP
  - CIEM

None of these approaches are fully satisfactory
Challenge: Shared Responsibility
Can lead to confusion and poor security controls

Non-Cloud

Access
To your services and your data.

Application
Your applications, code, configuration and deployment.

Virtual Services
Your Compute, Storage and Networks.

Multi Cloud
IaaS Tenant Responsible

Security of Access to Tenant’s Service and Data

- Security of Managed Container Registry, Images and Runtime
- Security of Tenant’s Application
- Security of Managed Kubernetes and Databases
- Security of Tenant’s own Kubernetes and Databases
- Security of Serverless and Cluster Infrastructure
- Security of Tenant’s Compute, Storage and Network
- Security of IaaS Service

CSP Responsible
Challenge: Privacy Enabled Data Protection
Exploiting and sharing data while ensuring security, privacy and compliance

Non-Cloud

**In Transit**
Across networks

**At Rest**
Everywhere – from end user device to cloud backup

**During Processing**
and while it is being shared and analyzed.

Multi Cloud
Challenge: Inconsistent Capabilities and Tools

Have led to an ad hoc approach to security and compliance

Ad Hoc Approach
Each cloud has own capabilities, tools, APIs and user interfaces

Identity
Data Protection
Vulnerability Management
Network Security
Inventory
Management

CASB
SASE
CIEM
CWPP
CAASM
CSPM

Multi Cloud

Identity
Data Protection
Vulnerability Management
Network Security
Inventory
Management

Non-Cloud
Desired Approach - Consistent Governance

For a mature approach to hybrid IT service delivery

**Consistent Governance Across the Hybrid Multi-Cloud**

Non-Cloud

- Identity
- Data Protection
- Vulnerability Management
- Network Security

Multi Cloud

- Identity
- Data Protection
- Vulnerability Management
- Network Security

CASB, SASE, CIEM, CWPP, CAASM, CSPM
Cloud Security Posture Management

What are the capabilities to look for?
Cloud Acronym Soup

What is CASB, CNAPP, CSPM, CWPP, CIEM, SASE?

**CASB**
- SaaS Cloud Inventory
- Control over unsanctioned SaaS
- Two control models
- Interwork with SaaS or Network controls
- Integrated DLP

**SASE**
- Network based cloud access control.
- Convergence of SWG, VPN, DNS, etc.
- Incorporates CASB functionality
- Zero Trust and micro-segmentation

**CIEM**
- Control over cloud infrastructure elements
- Virtual Resources have entitlements
- These are invisible and can be misused
- Visibility and Control

**CNAPP / CWPP**
- Protection of the DevOps cloud
- Container based workloads
- Serverless cloud
- Visibility and Control
- Over VMs, Containers and Serverless
**GRC vs Cloud Security Posture Management**

Terms change but objectives are similar

---

Non-Cloud

**Grandpa’s Risk and Compliance**

- Management
- Inventory
- Identity
- Network Security
- Vulnerability Management

**Static Controls**

- CASB
- SASE
- CIEM
- CWPP
- CAASM
- CSPM

---

Multi Cloud

**Cloud Security Posture Management**

- Management
- Identity
- Data Protection
- Network Security
- Vulnerability Management

**Dynamic Guardrails**

Ad Hoc Approach

Each cloud has own capabilities, tools, APIs and user interfaces.
Cloud Security Posture Management Dashboard

Every good solution should provide a dashboard!

To enable the organization to visualize the security and compliance of their use of cloud services.
Cloud Security Posture Management Capabilities
What a CSPM solution should offer

Eight Major Areas:
• Basic functionality
• User Risks
• Data Risks
• Network Risks
• Compute Risks
• DevOps Risks
• Risk Reporting
• Compliance Support
### Basic Capabilities
For Cloud Security Posture Management

<table>
<thead>
<tr>
<th>Inventory</th>
<th>Visibility</th>
<th>Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Of what needs to be governed:</td>
<td>Of security and compliance of cloud assets:</td>
<td>Policy based controls for cloud assets:</td>
</tr>
<tr>
<td>▪ Services</td>
<td>▪ Against Policy</td>
<td>▪ Enforce</td>
</tr>
<tr>
<td>▪ Service elements</td>
<td>▪ Against best practices</td>
<td>▪ Remediate</td>
</tr>
<tr>
<td>▪ In use and owned</td>
<td>▪ Against regulations</td>
<td>▪ Report</td>
</tr>
</tbody>
</table>
User and Entitlement Risks
Cloud Administrators and Cloud Infrastructure

Weak AuthN
Protect against account takeover:
- Weak authentication
- Compromised credentials
- Unused / orphan accounts.

Excessive Privilege
Limit scope of attack / misuse:
- Least privilege
- Separation of Duties
- Audit / Attestation

Infrastructure
Limit attack paths and technical exploits:
- Service elements
- Least privilege
- Activity monitoring
**Data Risks**

Data held and processed in the cloud service

---

### What Data

Protect data according to its sensitivity:

- Public data
- Regulated data
- Sensitive / Confidential data

---

### How Secured

Limit impact of unauthorized access:

- Exposed to the internet.
- Encrypted to policy
- Backed up

---

### Where held

Meet Legal and Regulatory obligations:

- Geographical location
- Cloud policy
- Appropriate controls
Network Risks
From virtual networks in the cloud services

Topology
Discover topology and control points:
- Range of Cloud Services
- AWS, Azure, Google, Oracle
- VMware, OpenStack, Hyper V

Configuration
Risks related to control point configurations:
- Routing vs Policy.
- Protocols vs Policy
- Zero Trust

Certificates
Risks related to the Certificate management
- Self-signed Certificates
- Weak encryption
- Certificate Root
Compute Service Risks
Virtual Servers in the cloud service

Virtual Servers
Cover Native Virtual Sever types for:
- Range of Cloud Services
- AWS, Azure, Google, Oracle
- VMware, OpenStack, Hyper V

Entitlements
Risks related to VM entitlements:
- Excessive privileges.
- Without an owner
- Dormant / not used

OS Config
Risks related to the OS set up:
- Known CVEs
- Missing Patches
- Root enabled
## DevOps Risks

Virtual Servers in the cloud service

### Coverage

- **Inventory of Kubernetes Clusters:**
  - Range of Cloud Services
  - AWS, Azure, Google, Oracle
  - Clusters, Pods, Containers

### Service Accounts

- **Risks related to Kubernetes entitlements:**
  - Excessive privileges.
  - Without an owner
  - Activity

### Vulnerabilities

- **Risks related to the Containers and Deployments:**
  - OS Images
  - 3rd Party Packages
  - Code scanning
  - Container Drift
### Detection, Reporting and Remediation

**Essential security controls**

<table>
<thead>
<tr>
<th>Financial Impact</th>
<th>Risk Score</th>
<th>Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td>The potential financial impact of the risk.</td>
<td>A configurable score for the risk.</td>
<td>Risk described in categories (High, medium, Low).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Laws / Regulations</th>
<th>Frameworks</th>
<th>Best Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>With predefined policies out of the box. (e.g., GDPR, HIPAA, TISAX, PCI/DSS)</td>
<td>Frameworks with policies provided out of the box. (e.g., ISO 27001, COBIT,)</td>
<td>Best practices with policies out of the box. (e.g., NIST, MITRE, CIS)</td>
</tr>
</tbody>
</table>
CSPM

GRC for the cloud?
Summary
Dynamic infrastructure and DevOps need Dynamic Controls and Governance.

**Digitalization increases Cyber Risks**
- Business Continuity
- Data Breaches
- Compliance failure

**Software Defined Infrastructure**
- Virtual
- Dynamic
- DevOps

**Dynamic Controls**
- Inventory.
- Entitlements.
- Vulnerabilities

**CSPM**
- Visualization
- Policy
- Best practices
- Compliance
THANKS!

Any questions?