粵港澳大灣區網絡安全協會
Greater Bay Area Cybersecurity Association

# 全球化视角下企业多云安全管控新思考与实践

Dylan 李磊

01/09

# 目錄

CONTENTS

# 众说多云

粵港澳大灣區網絡安全協會
Greater Bay Area Cybersecurity Association

**Azure**

Multicloud is the practice of using the services of **multiple cloud providers** to optimize workload performance, increase flexibility, and mitigate the risks of relying on any one vendor.

**GCP**

Multicloud is when an organization uses cloud computing services from at least **two** cloud providers to run their applications. multicloud environments typically include a combination of two or more **public clouds**, two or more **private clouds**, or some combination of **both**

Gartner®

Multicloud is using **two clouds** for **similar services**. If you use Salesforce and AWS, that counts as one SaaS and one IaaS – not multiple clouds. But running VMs or K8s in Azure and AWS means you're a multiclouder.

# 多云的定义

粵港澳大灣區網絡安全協會
Greater Bay Area Cybersecurity Association

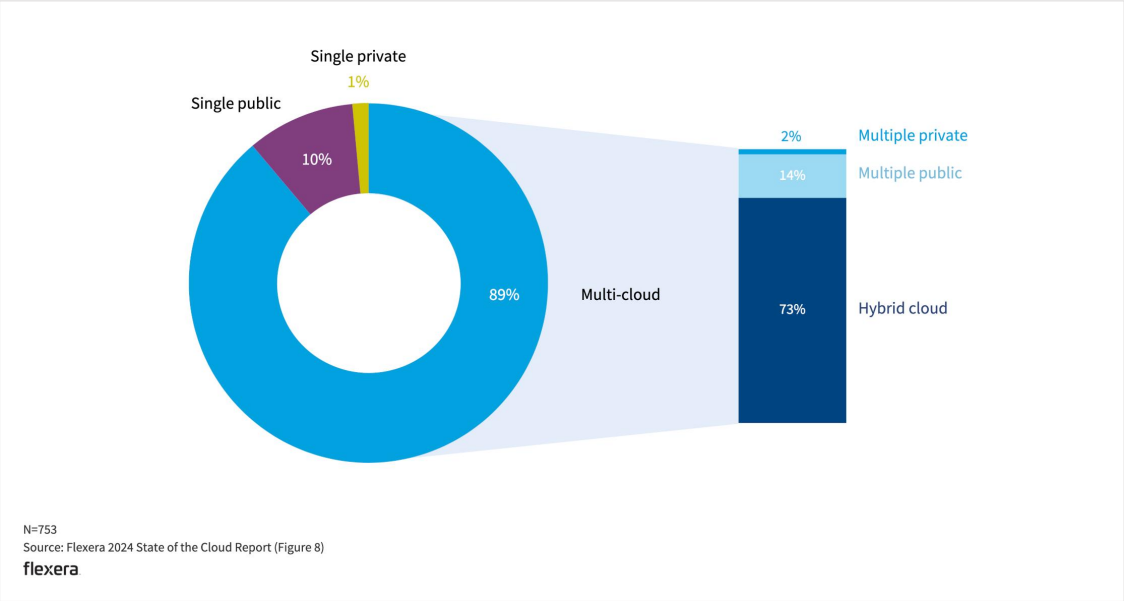
**ISO/IEC 22123:**multi-cloud is a cloud **deployment model** in which a customer uses **public cloud** services provided by **two or more** cloud service providers


A multi-cloud can also be a hybrid cloud, and a hybrid cloud can also be a multi-cloud

# 多云是趋势

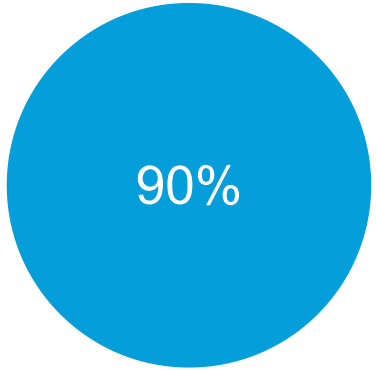
粵港澳大灣區網絡安全協會
Greater Bay Area Cybersecurity Association

## 众多组织拥抱多云




2024 State of the Cloud Report
by Flexera

## 亚太企业拥抱多云




Asia/Pacific State of Cloud: Adoption Trends,
Challenges, and Preferences
By IDC

# 多云面临的安全挑战

# 云与IDC差异



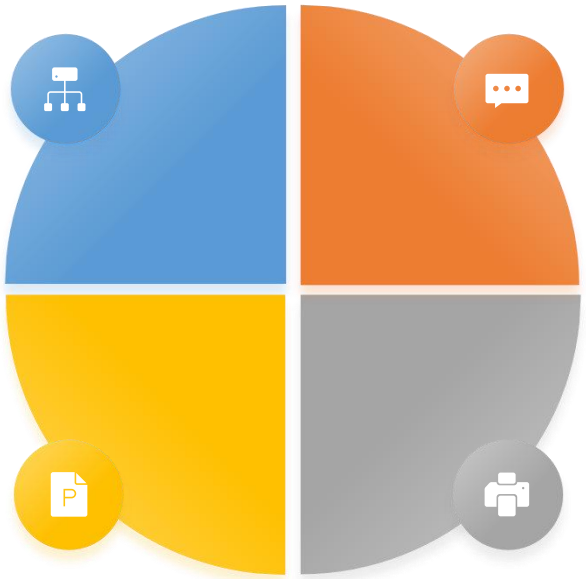
典型差异性的存在，需要我们以全新视角来对待云安全

## 云原生化

- 专属概念和产品：容器、微服务、K8S等
- 基建变化：IAAS、PAAS、SAAS

## 产品灵活化

- 使用便捷，多角度支持，没有做不到，只有想不到



## 安全属性化

- 除云产品功能外，多数附带安全功能，常见的如权限控制、IP控制

## 边界多样化

- 任何产品都有可能成为云上网络安全边界。如ECS

# 单云面临的安全挑战

粤港澳大灣區網絡安全協會
Greater Bay Area Cybersecurity Association

拿来即用？云产品自身安全性FW、OSS、FC、OB、DW、waf

云产品权限精细化管控的复杂度

安全/SRE/网络等


数据泄露和攻击风险面变大（云产品任何地方任何时间都可访问）

典型云化新特性RAM/AK的问题（RAM 、主账号AK、超管权限AK）

# 多云面临的安全挑战



**01**

**复杂度**

- 不同云的架构和形态不一
- 安全控制
- 管理工具

(如PRAM、ARAM)

**02**

**攻击面**

- 双非“风险
- 权限风险
- 配置风险

**03**

**人**

- 熟悉多云的安全人才稀缺
- 技能：出事如何响应和排查

**04**

**合规**

满足不同区域数据保护法律要求

# 多云新思考

## 云服务商

AWS/Azure/
GCP/阿里云

## 云产品不一

云产品名称，
云产品能力

## 云的架构

Xen虚拟化
KVM虚拟化
Hyper-V虚拟化

# 多云产品对比一览



| ON-PREMISES | AZURE | AWS | GOOGLE | ORACLE | IBM | ALIBABA | TENCENT |
|---|---|---|---|---|---|---|---|
| Firewall & ACLs | Azure Firewall Network Security Groups | AWS Network Firewall AWS Network ACLs | VPC Firewall | SmartNIC Oracle CloudGuard | Virtual Router Appliance | Cloud Firewall | VPC Network ACLs Security Groups |
| IPS/IDS | Azure Firewall | AWS Network Firewall Amazon Detective | | | | Cloud Firewall | Cloud Workload Protection |
| Web Application Firewall (WAF) | Azure Web Application Firewall (WAF) | AWS WAF AWS Firewall Manager | Cloud Armor WAF | Oracle WAF | Cloud Internet Services | Cloud WAF | Web Application Firewall |
| SIEM & Log Analytics | Azure Sentinel | Amazon Detective Security Hub/GuardDuty | Chronicle Backstory Event Threat Detection | Oracle Security Monitoring and Analytics | Cloud Log Analysis Cloud Activity Tracker | Log Analysis | Security Operations Center |
| Data Loss Prevention (DLP) | Azure Inf. Protection M365 Compliance Center | Amazon Macie | Cloud Data Loss Prevention API | | | Web Application Firewall | |
| Key Management | Azure Key Vault | Key Management Service AWS Secrets Manager | Cloud Key Management Service | Cloud Infrastructure Key Management | Key Protect Cloud Security | Key Management Service (KMS) | Secrets Manager Key Management Service |
| Encryption At Rest | Storage Encryption for Data at Rest | EBS/EFS Volume Encryption, S3 SSE | Google Cloud Platform (native) | Cloud Infrastructure Block Volume | Hyper Protect Crypto Services | Data Encryption Service | Key Management Service (Beta) |
| DDoS Protection | Azure DDoS Protection | AWS Shield | Cloud Armor | Built-in DDoS defense | | Anti-DDoS | Anti-DDoS |
| SSL Decryption Reverse Proxy | Application Gateway | Application Load Balancer | HTTPS Load Balancing | | Cloud Load Balancer | | |
| Certificate Management | Azure Key Vault | AWS Certificate Manager | Secret Manager Cloud Key Management | | Certificate Manager | Cloud SSL Certificates Service | |
| Container Security | Azure Defender | Amazon EC2 Container Service (ECS) | Kubernetes Engine | Oracle Container Services | Containers - Trusted Compute | Container Registry | |
| Identity and Access Management | Azure Active Directory PIM | Identity and Access Management (IAM) | Cloud IAM | Oracle Cloud Infrastructure IAM | Security Verify | Resource Access Management (RAM) | Tencent Cloud Organization |
| Privileged Access Management (PAM) | Azure AD Privileged Identity Management | | | | Security Verify | | |
| Multi-Factor Authentication (MFA) | Azure MFA | AWS MFA (part of AWS IAM) | Titan Security Key | Oracle Cloud Infrastructure IAM | Security Verify | Resource Access Management (RAM) | |
| Centralized Logging / Auditing | Azure Monitor Azure Sentinel | CloudWatch / S3 bucket | Stackdriver Mon / Logging Access Transparency | Oracle Cloud Infrastructure Audit | Log Analysis with LogDNA | ActionTrail | Flow Logs |
| Load Balancer | Azure Load Balancer | Application Load Balancer Classic Load Balancer | Cloud Load Balancing HTTPS Load Balancing | Cloud Infrastructure Load Balancing | Cloud Load Balancer | Server Load Balancer (SLB) | Cloud Load Balancer |
| LAN | Virtual Network | Virtual Private Cloud (VPC) | Virtual Private Cloud Network (VPC) | SmartNIC | VLANs | Virtual Private Cloud (VPC) | Virtual Private Cloud (VPC) |
| WAN | ExpressRoute | Direct Connect | Dedicated Interconnect | FastConnect | Direct Link | VPN Gateway Express Connect | Direct Connect (DC) |
| VPN | Azure Virtual Network Gateway | VPC Customer Gateway AWS Transit Gateway | Google VPN | Dynamic Routing Gateway (DRG) | IPSec VPN Secure Gateway | VPN Gateway | VPN Connection |
| Governance Risk and Compliance Monitoring | Azure Security Center M365 Compliance | AWS Security Hub AWS Compliance Center | Cloud Security Command Center | | Cloud Security & Compliance Center | ActionTrail | CloudAudit |
| Backup and Recovery | Azure Backup Azure Site Recovery | AWS Backup CloudEndure DR | Object Versioning Cloud Storage Nearline | Archive Storage | Cloud Backup | Hybrid Backup Recovery | |
| Vulnerability Assessment | Azure Defender Azure Security Center | Amazon Inspector AWS Trusted Advisor | Cloud Security Scanner | Security Vulnerability Scanning Service | Cloud Security Advisor Vulnerability Advisor | PenetrationTest Website Threat Inspector | Cloud Workload Protection |
| Patch Management | Azure ARC Update Management | AWS Systems Manager | | Risk Management Cloud | IBM Cloud Orchestrator | | |
| Change Management | Azure Automation Change Tracking and Inventory | AWS Config | | | | Application Configuration Management (ACM) | |
| IoT Security | Azure Defender for IoT | AWS IoT Device Defender | Edge TPU IoT Core | | Watson IoT Platform Edge Application Manager | IoT Platform Link IoT Edge | |
| Extended Storage | Azure Data Explorer (ADX) Azure Log Analitics | Amazon S3 Glacier | Cloud Storage for Data Archiving | Archive Storage | Cloud Block Storage | Log Service | |
| Secure Operation & Management | Azure Bastion | | Google Cloud Operation Suite ( form. Stackdriver) | OCI Bastion | | BastionHost | |
| Application Security | | Amazon Inspector | | | | | Mobile Security |
| Email Protection | Defender for Office 365 | | Various controls embedded in G-Suite | | | | |
| Antimalware | Azure Defender | | | | | Threat Detection Service (TDS) | |
| Endpoint Protection | Defender For Endpoint Azure Defender | | Shielded VM | | | Server Guard | |
| File Integrity Monitoring (FIM) | Azure Defender | | Shielded VM | | | | |
| Cloud Access Security Broker (CASB) | Microsoft Cloud App Security (MCAS) | | | Oracle CASB | | | |

Mapping of On-Premises Security Controls vs Major Cloud Providers Version 5.0 July 2021 © Adrian Grigorof, Marius Mocanu
High Definition available at http://www.managedsentinel.com

# 变与不变

粤港澳大灣區網絡安全協會
Greater Bay Area Cybersecurity Association

云的**特性**
没有变

云与IDC
**典型差异**没有变

云**风险管理**
**逻辑**没有变

# 云安全管控框架OCBC

粤港澳大灣區網絡安全協會
Greater Bay Area Cybersecurity Association

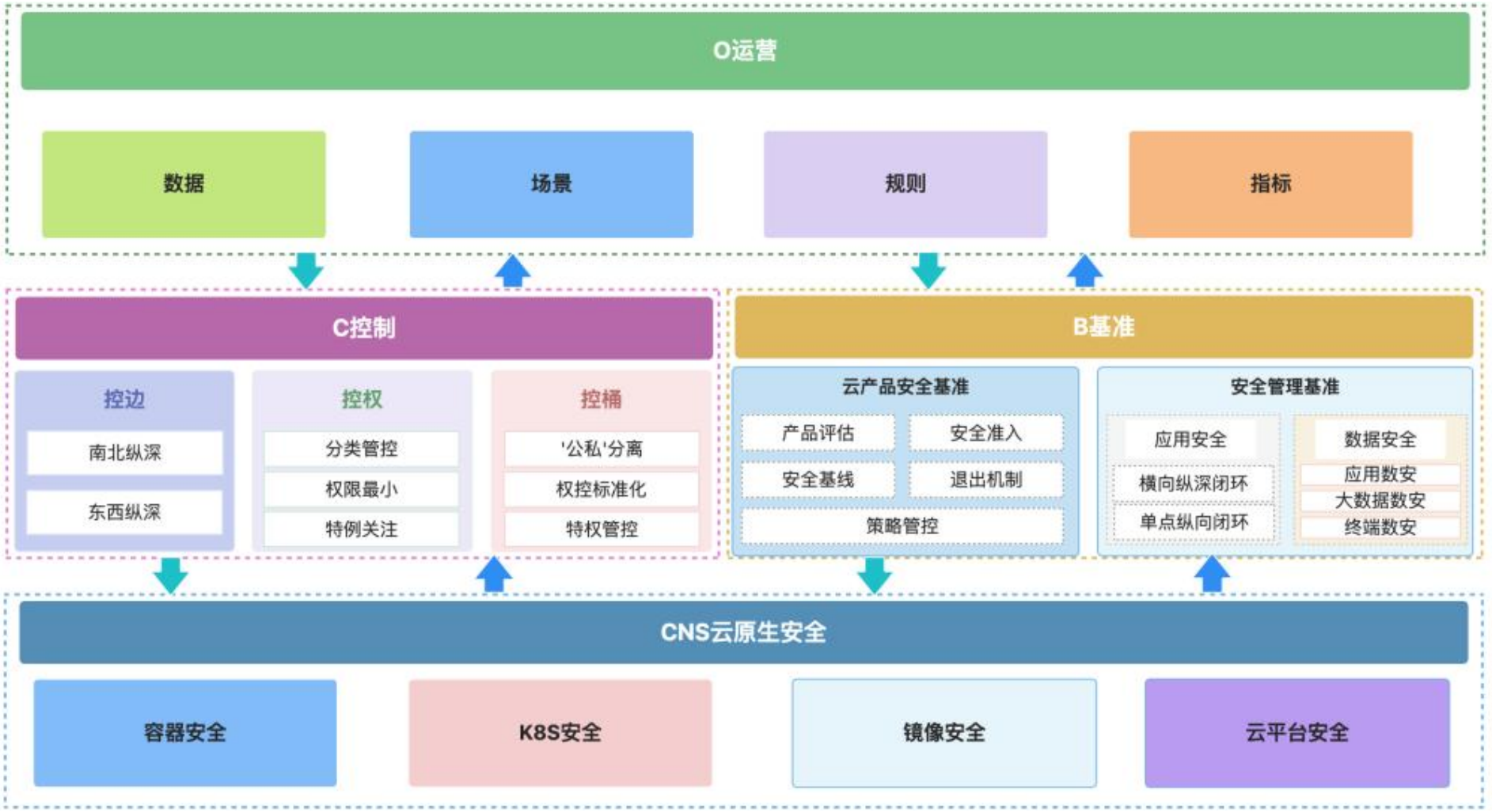
1. 云上安全管理框架，22年发布，具备指引性强、落地性强的特点
2. 在多国多地区公有云、金融业务站点落地实践，经历了多次内、外部红蓝演练、众测、iCAST等检验其价值


关注公众号“粤港澳大湾区网络安全协会”查看更多关于OCBC框架更详细解读

# 云安全管控框架OCBC



- **O**peration 运营
- **C**ontrol 控制
- **B**aseline 基准
- **C**loud Native Security 云原生安全



# 多云实践

# 基于OCBC框架下的多云分层管理

粤港澳大灣區網絡安全協會
Greater Bay Area Cybersecurity Association

**【重管控】金融级安全**

基于OCBC框架下，落地纵深防护体系

多云核心站点

**O运营**

数据 | 场景

规则 | 指标

**C控制**

控边

控权

控桶

**B控制**

云产品安全基准

安全管理基准

**CNS云原生安全**

容器 | 镜像 | K8S

云平台安全

**【轻管控】低保级安全**

基于权限为管控核心，以边界+基线巡检+威胁检测为兜底

多云非核心站点


**公有云安全4平台**

阿里云

谷歌云

亚马逊

Bosten

权限

NAPA 风险运营

Merlion 威胁检测+基线检测

Kanas 资产

# 结语



**01 不现实**

希望单纯依赖云产品构建云上安全管控体系是不现实的

**02 不可取**

所有云产品拿来即用的思路也是不可取的。同时，希望引入三方非云平台安全产品需要考虑云平台环境的融入性和复杂度

**03 第一责任人**

每家云平台都可能存在安全漏洞，只是存在多与少、发现早与晚的问题。但是，更多的时候，其实是作为甲方企业没有安全、合规的使用云而造成的安全漏洞或数据泄露，云平台间接成了”背锅侠“。所以，坚持做好用云安全第一责任人的角色定位是重要的

**04 主动补位**

云上OCBC安全管控框架中的C控制控权控桶天然具备安全属性，单纯的管理要求或职责转嫁，安全始终会处于一个被动收拾的角色，建议安全团队主动承担或提供标准的平台化安全能力支撑

粵港澳大灣區網絡安全協會
Greater Bay Area Cybersecurity Association

# CONTACT INFORMATION
# 聯繫我們

## 粵港澳大灣區網絡安全協會

粵港澳唯一一個以促進網絡安全、數據安全和監管合規交流、加強粵港澳安全信息、安全技術、安全人才互通與融合、向粵港澳青少年宣傳推廣網絡安全意識、搭建三地企業間溝通平台、推動粵港澳三地及海外交流的組織。

行業動態 | 在線社區 活動預告 招聘資訊

Wechat關注我們

Wechat添加好友

粵港澳大灣區網絡安全協會
Greater Bay Area Cybersecurity Association

# THANKS