
aws
INNOVATE
ONLINE CONFERENCE

aws INNOVATE
ONLINE CONFERENCE

分会场六：信息安全

启动上云的安全风险和最佳实践

朱志强，AWS 资深云安全拓展经理

目录

1. 客户为什么选择亚马逊云计算
2. ATT & CK 攻防架构与云安全威胁
3. 亚马逊云安全体系
4. 最佳安全实践

1. 客户为什么选择亚马逊云计算

AWS 中国（宁夏）区域由西云数据运营
AWS 中国（北京）区域由光环新网运营

aws INNOVATE
ONLINE CONFERENCE

亚马逊云计算优势

安全性

AWS 的安全性始于我们的核心基础设施。我们的基础设施针对云定制，旨在满足全球最为严格的安全要求，处于全天候监控之下，从而帮助确保您数据的机密性、完整性和可用性。在我们的数据中心和区域互连的 AWS 全球网络中，所有的数据流动在离开我们的安全设施之前，都经过物理层自动加密。您可以在最安全的全球基础设施上进行构建，知道您始终控制自己的数据，并且能够随时加密、移动以及管理保留这些数据。

可用性

AWS 提供所有云提供商中最高的网络可用性，停机时间比第二大云提供商少 7 倍。*每个区域都完全隔离并且由多个可用区组成，各可用区是与基础设施完全隔离的分区。为了更好地隔离任何问题并实现高可用性，您可以跨同一区域中的多个可用区对应用程序进行分区。可用区专为实现物理冗余而设计，具有弹性，即使在出现断电、互联网停机、洪水和其他自然灾害的情况下也能实现不间断的性能。

性能

AWS 全球基础设施为性能而构建。AWS 区域提供低延迟、低数据包丢失和较高的整体网络质量。这通过完全冗余的 100 GbE 光纤骨干网实现，通常在区域之间提供多 TB 容量。AWS 本地区域和 AWS Wavelength 与我们的电信提供商合作，通过提供更接近最终用户的 AWS 基础设施和服务以及 5G 连接设备为需要个位数毫秒级延迟的应用程序提供性能。无论您的应用程序需要什么，您都可以根据需要快速启动资源，在几分钟内部署数百甚至数千台服务器。

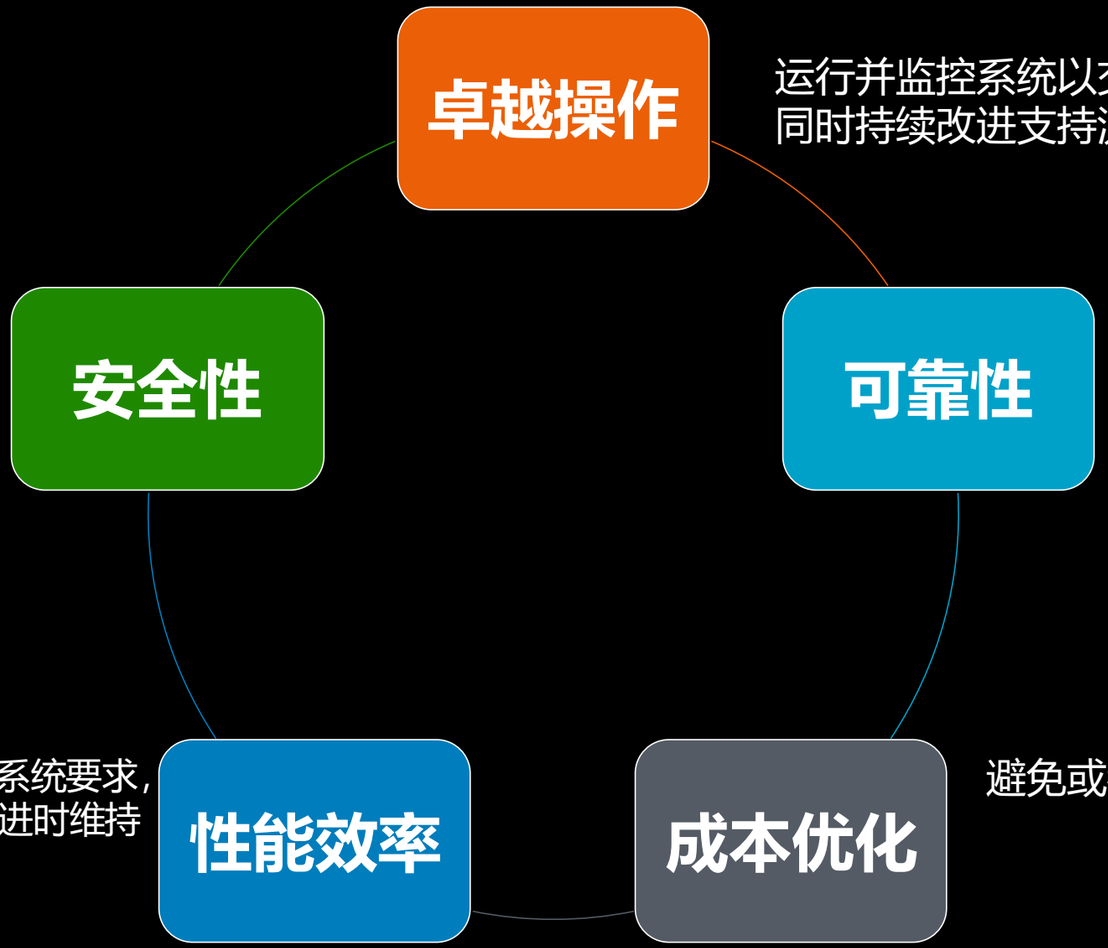
AWS 中国（宁夏）区域由西云数据运营
AWS 中国（北京）区域由光环新网运营

AWS 让客户获益

- AWS 基础架构旨在提供一个高度可扩展，高度可靠的平台，使客户能够快速安全地部署应用程序和数据。所有 AWS 客户都将从为满足我们对安全性最强的客户的要求而构建的数据中心和网络架构中受益。 AWS 提供了网络安全功能，以增加隐私并控制网络访问，清单和配置管理，以使您快速行动，同时仍可确保您的云资源符合组织标准和最佳实践。
- 通过在经过认可的环境中进行操作，客户可以减少他们需要执行的审计范围和成本，因为不断对 AWS 计算环境进行审计，以帮助客户确定其在 AWS 上运行的环境的合规性。
- AWS 云使客户可以在保持安全环境的同时进行扩展和创新。客户只为使用的服务付费，这意味着您可以获得所需的安全性，而无需支付前期费用，并且成本比本地环境低。

AWS 中国（宁夏）区域由西云数据运营
AWS 中国（北京）区域由光环新网运营

AWS 良好架构框架（五大支柱）



运行并监控系统以交付商业价值，同时持续改进支持流程与规程的能力。

系统从基础设施或者服务故障当中实现恢复、以动态方式获取计算资源以满足需求，以及缓解配置错误或者暂时性网络问题等干扰因素的能力。

避免或者消除不必要成本或者欠佳资源的能力。

高效利用计算资源以满足系统要求，同时在需求变更及技术演进时维持这种效率水平的能力。

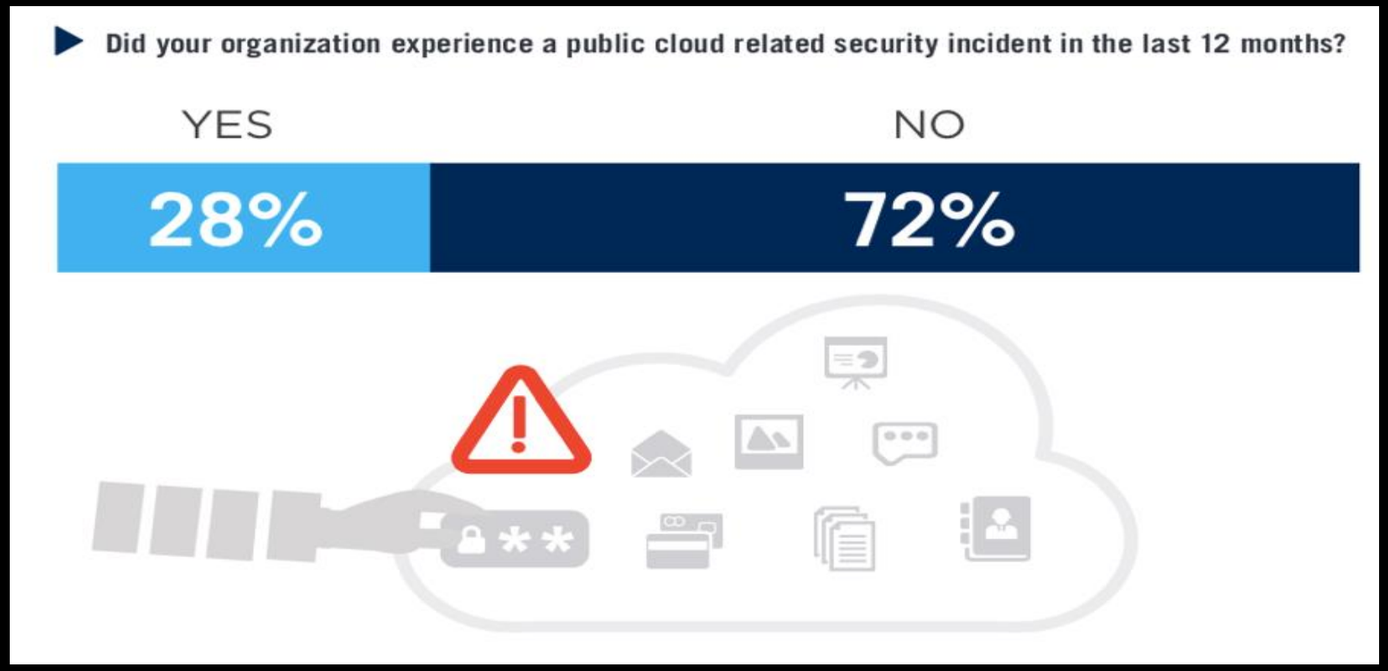
在交付商业价值的同时，通过风险评估与缓解策略保护信息系统以及资产的能力。

AWS 中国（宁夏）区域由西云数据运营
AWS 中国（北京）区域由光环新网运营

2. 云安全威胁和 ATT & CK 攻防架构

云安全威胁调查

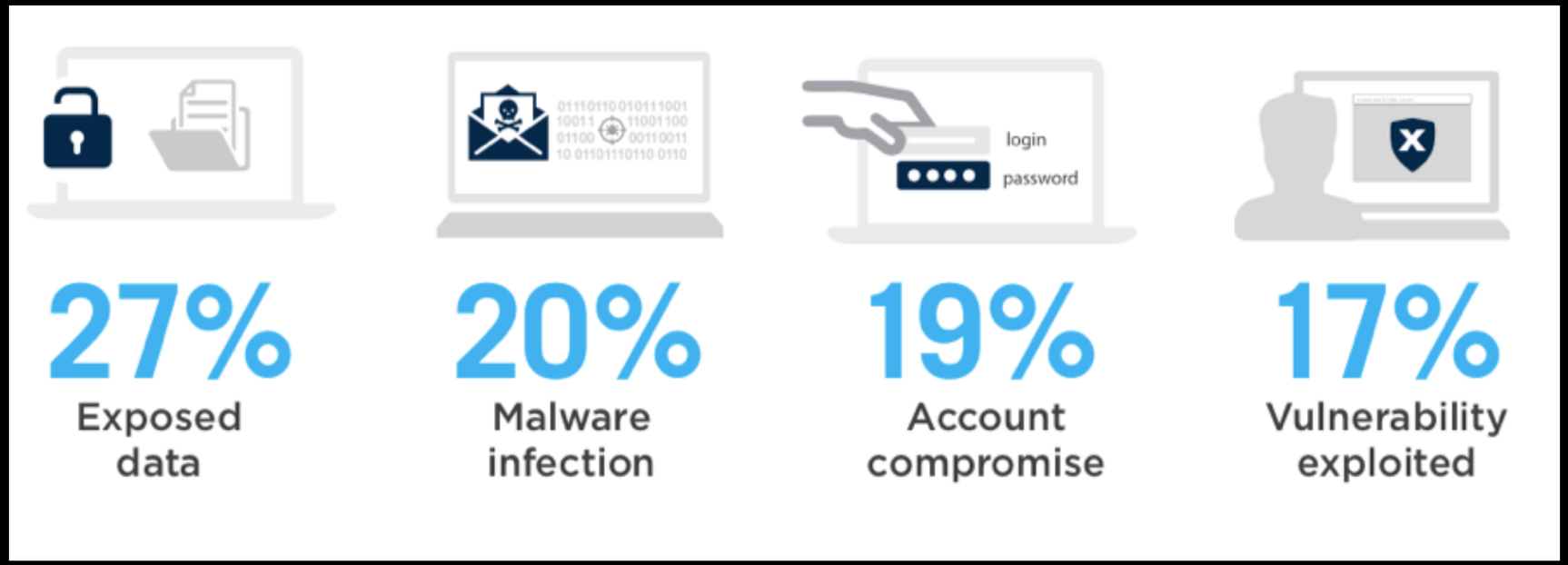
在过去的 12 个月中，28% 被调查的组织确认他们遇到了云安全事件。但是，这并不意味着云安全事件只有这些。因为另一组调查数据也表明，25% 的组织并不知道其运行在云中的数据或业务是否被破坏，只有 15% 的组织确认了云安全事件，这意味着，有大量的云安全威胁或事件仍然潜藏在组织的视界之外。



AWS 中国（宁夏）区域由西云数据运营
AWS 中国（北京）区域由光环新网运营

云安全事件

在这些云安全事件中，数据泄露（27%）位居榜首，其次是恶意软件感染（20%）和帐户受损（19%）。同时，在网络安全专业人员最关心的云安全问题中，数据丢失和泄漏以 64% 的比例位居首位，这意味着防范数据泄露是现阶段云安全防护最重要的任务之一。



AWS 中国（宁夏）区域由西云数据运营
AWS 中国（北京）区域由光环新网运营

企业上云会面临哪些安全威胁

上云初期	业务增长期	业务平稳期
• 身份凭证和访问管理不足 • 不安全的接口和 API • 主机安全 • 系统漏洞 • 安全审查 • 数据泄漏	• 帐户劫持 • 恶意内部人士 • 高级持续性威胁 • 数据丢失 • 尽职调查不足 • 滥用和恶意使用云服务 • 拒绝服务 • 共享技术漏洞 • 合规	• 帐户劫持 • 恶意内部人士 • 高级持续性威胁 • 数据丢失 • 尽职调查不足 • 滥用和恶意使用云服务 • 拒绝服务 • 共享技术漏洞 • 大数据安全 • 合规

AWS 中国（宁夏）区域由西云数据运营
AWS 中国（北京）区域由光环新网运营

AWS ATT&CK 云攻击模型

Initial Access 初始访问	Execution 执行	Persistence 持久化	Privilege Escalation 提升权限	Defense Evasion 防御绕过	Credential Access 凭据访问	Discovery 发现	Lateral Movement 横向移动	Vertical Movement 纵向移动	Collection 收集	Exfiltration 数据泄露	Impact 影响
Exploit Public-Facing Application	Lambda Functions	IAM Group Manipulation	Golden SAML	Connection Proxy	Brute Force	Cloud Service Dashboard	Cross Account Roles (IAM AssumeRole)	Cloud to Network	Automated Collection	Exfiltration from S3	Distributed Denial of Service Attack
Supply Chain Compromise	SSM Agent	IAM Role Manipulation	IAM Group Manipulation	Disabling Security Controls	Cloud Instance Metadata API	Cloud Service Discovery	Takeover Parent AWS Account Ownership	Network to Cloud	Data from Cloud Storage Service	Exfiltration from SageMaker	Resource Hijacking
Trusted Relationship		IAM User Manipulation	IAM Policy Manipulation	IAM User and Role Hopping	Credentials in Files	IAM Discovery			Data from Information Repositories	Transfer Data to Cloud Account	
Valid Accounts		IAM Policy Manipulation	IAM Role Manipulation	Modify Jupyter Notebook		Network Service Scanning			Data from Local System		
		Implant Container Image	IAM User Manipulation	Multi-hop Proxy		Network Share Discovery			Data Staged		
		Modify AWS Service	Valid Accounts	Operation Rate Control		Remote System Discovery					
		Modify Jupyter Notebook		Region Selection and Hopping		System Information Discovery					
		New AWS Service		Revert Cloud Instance		System Network Configuration Discovery					
		Redundant Access		Unused/Unsupported Cloud Regions		System Network Connections Discovery					
		Trusted Relationship		User Agent Spoofing and Randomization							
		Valid Accounts		Valid Accounts							

3.亚马逊云安全体系

AWS 中国（宁夏）区域由西云数据运营
AWS 中国（北京）区域由光环新网运营

aws INNOVATE
ONLINE CONFERENCE

AWS 和客户共同承担安全责任

客户内容

平台, 应用, 认证 & 访问管理

操作系统,、网络 & 防火墙设置

客户端数据加密 | 服务器端数据加密 | 网络流量保护

客户负责云业务安全

AWS 基础服务

计算 | 存储 | 数据库 | 网络

AWS 全球基础设施

可用区

区域

边缘节点

AWS 负责云设施安全

AWS 中国（宁夏）区域由西云数据运营
AWS 中国（北京）区域由光环新网运营

AWS 云防护理念

安全控制 4 象限

安全防护 5 核心
认证和访问管理
监测控制
基础设施安全
数据保护
事件响应

防护加强5核心				
安全运营和开放	合规验证	弹性	配置和漏洞分析	安全大数据分析

AWS 中国（宁夏）区域由西云数据运营
AWS 中国（北京）区域由光环新网运营

AWS 安全解决方案

认证 & 访问管理

AWS Identity & Access Management (IAM)

AWS Single Sign-On

AWS Directory Service

Amazon Cognito

AWS Organizations

AWS Secrets Manager

AWS Resource Access Manager

监测控制

AWS Security Hub

Amazon GuardDuty

AWS Config

AWS CloudTrail

Amazon CloudWatch

Amazon VPC Flow Logs

基础设施防护

AWS Systems Manager

AWS Shield

AWS WAF – Web application firewall

AWS Firewall Manager

Amazon Inspector

Amazon Virtual Private Cloud (VPC)

数据保护

AWS Key Management Service (KMS)

AWS CloudHSM

AWS Certificate Manager

Amazon Macie

事件响应

AWS Config Rules

AWS Lambda

AWS 中国（宁夏）区域由西云数据运营
AWS 中国（北京）区域由光环新网运营

AWS 基础和分层安全服务

AWS Security Hub
AWS Organizations
AWS Control Tower
AWS Trusted Advisor

AWS Transit Gateway
Amazon VPC
AWS IoT Device Defender
Amazon Cloud Directory
Amazon VPC PrivateLink
AWS Direct Connect
Resource Access manager
AWS Directory Service

Amazon GuardDuty
Amazon Macie
Amazon Inspector
AWS Security Hub

Amazon CloudWatch
AWS Step Functions
AWS Systems Manager
AWS Lambda

AWS OpsWorks
AWS CloudFormation

认证 → 防护 → 监测 → 响应 → 恢复

自动化
深入调查

AWS Service Catalog
AWS Config
AWS Well-Architected Tool
AWS Systems Manager

AWS Shield
AWS IAM
AWS Secrets Manager
AWS KMS
Amazon Cognito
AWS WAF
AWS Firewall Manager
AWS Certificate Manager
AWS CloudHSM
AWS Single Sign-On

Amazon Detective
Amazon CloudWatch
AWS CloudTrail
AWS Personal Health Dashboard
Amazon Route 53

Amazon S3 Glacier
Snapshot
Archive

AWS 中国（宁夏）区域由西云数据运营
AWS 中国（北京）区域由光环新网运营

全局安全性和合规性控制

AWS 中国（宁夏）区域由西云数据运营
AWS 中国（北京）区域由光环新网运营

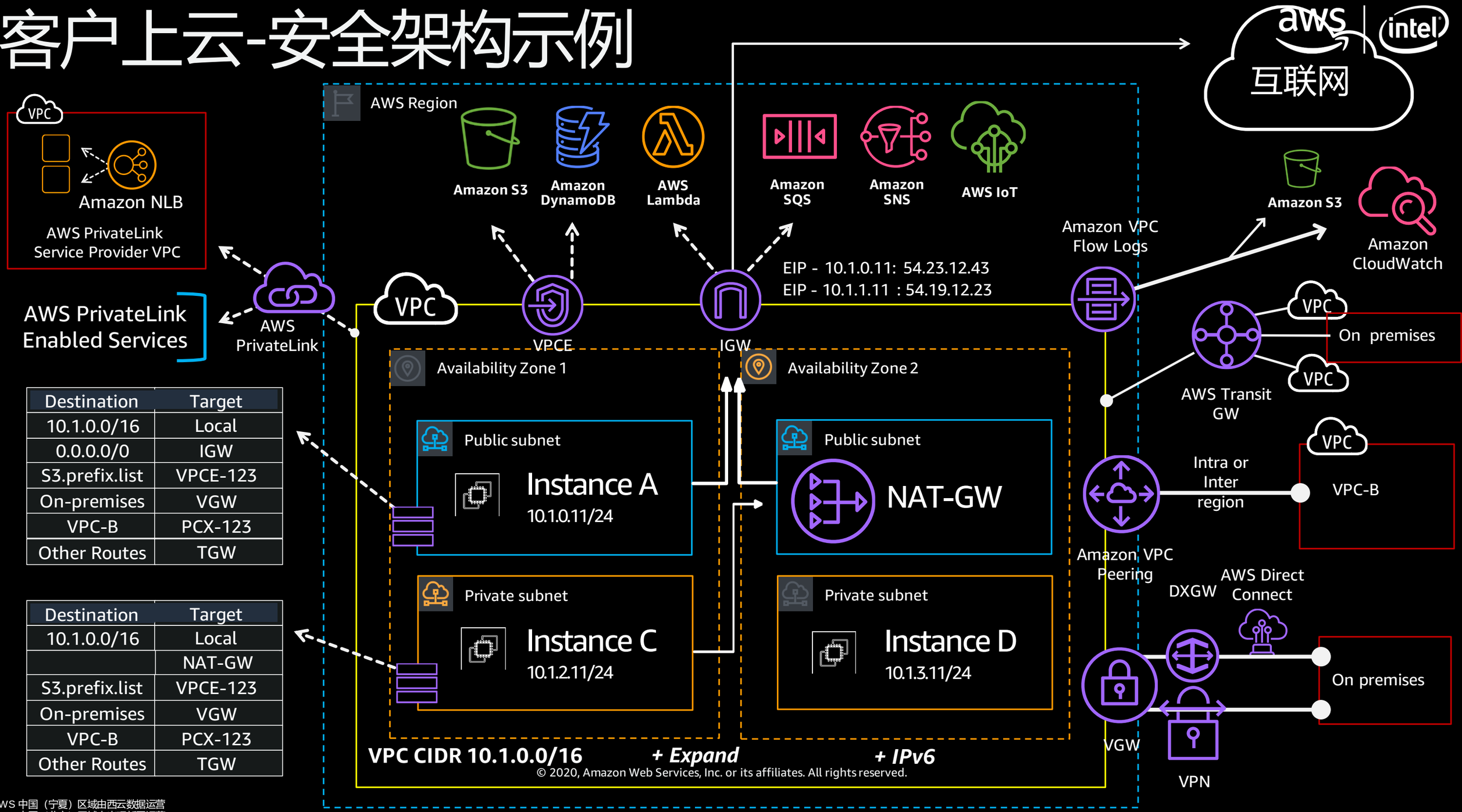
安全服务全球合作伙伴体系

APN 合作伙伴提供了数百种行业领先的产品，这些产品与本地环境中的现有控件等效相同或集成。 这些产品是对现有 AWS 服务的补充，使您能够在云和本地环境中部署全面的安全架构和更无缝的体验。

AWS 中国（宁夏）区域由西云数据运营
AWS 中国（北京）区域由光环新网运营

4. 最佳安全实践

客户上云-安全架构示例

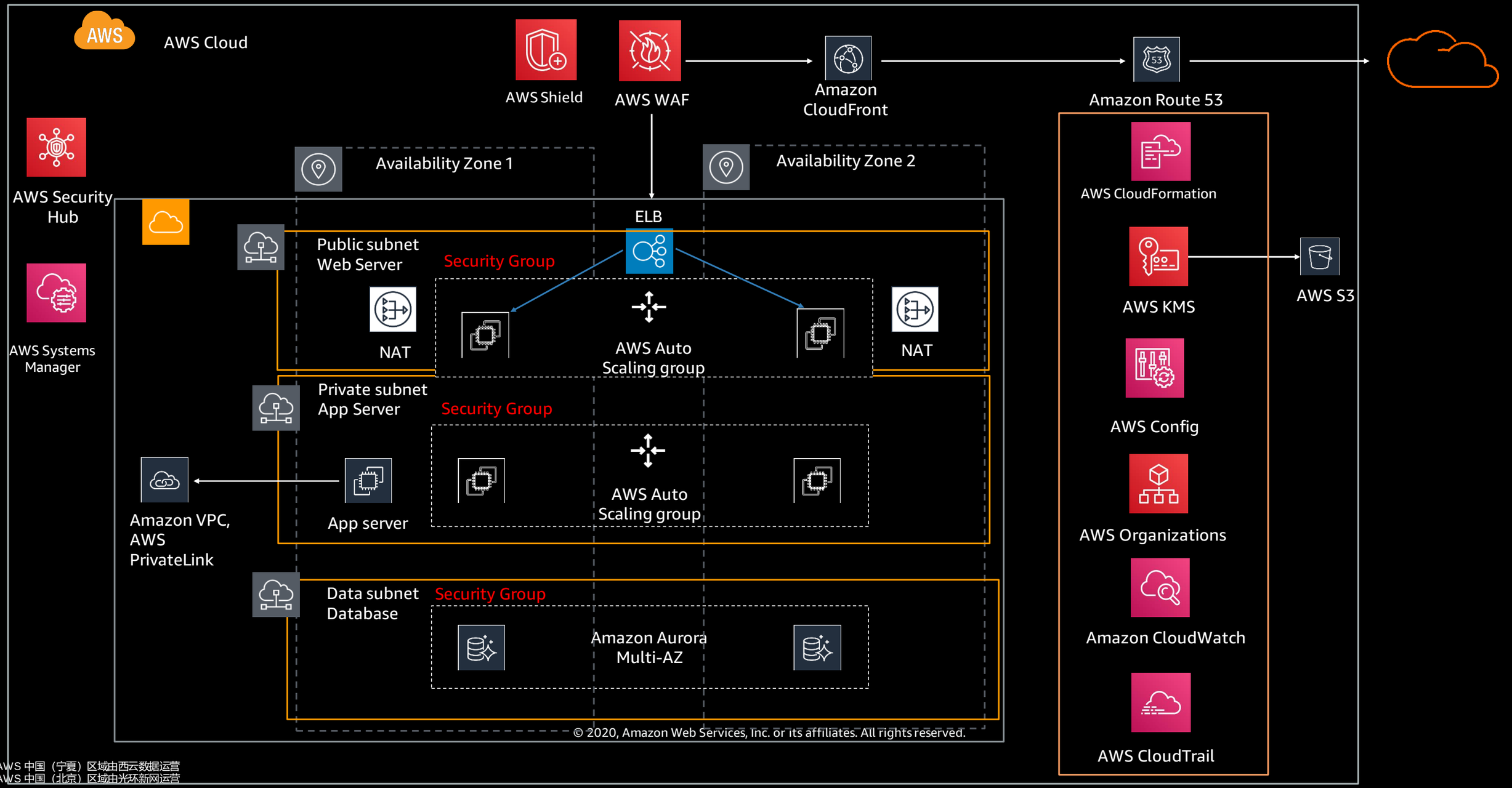


Destination	Target
10.1.0.0/16	Local
0.0.0.0/0	IGW
S3.prefix.list	VPCE-123
On-premises	VGW
VPC-B	PCX-123
Other Routes	TGW

Destination	Target
10.1.0.0/16	Local
	NAT-GW
S3.prefix.list	VPCE-123
On-premises	VGW
VPC-B	PCX-123
Other Routes	TGW

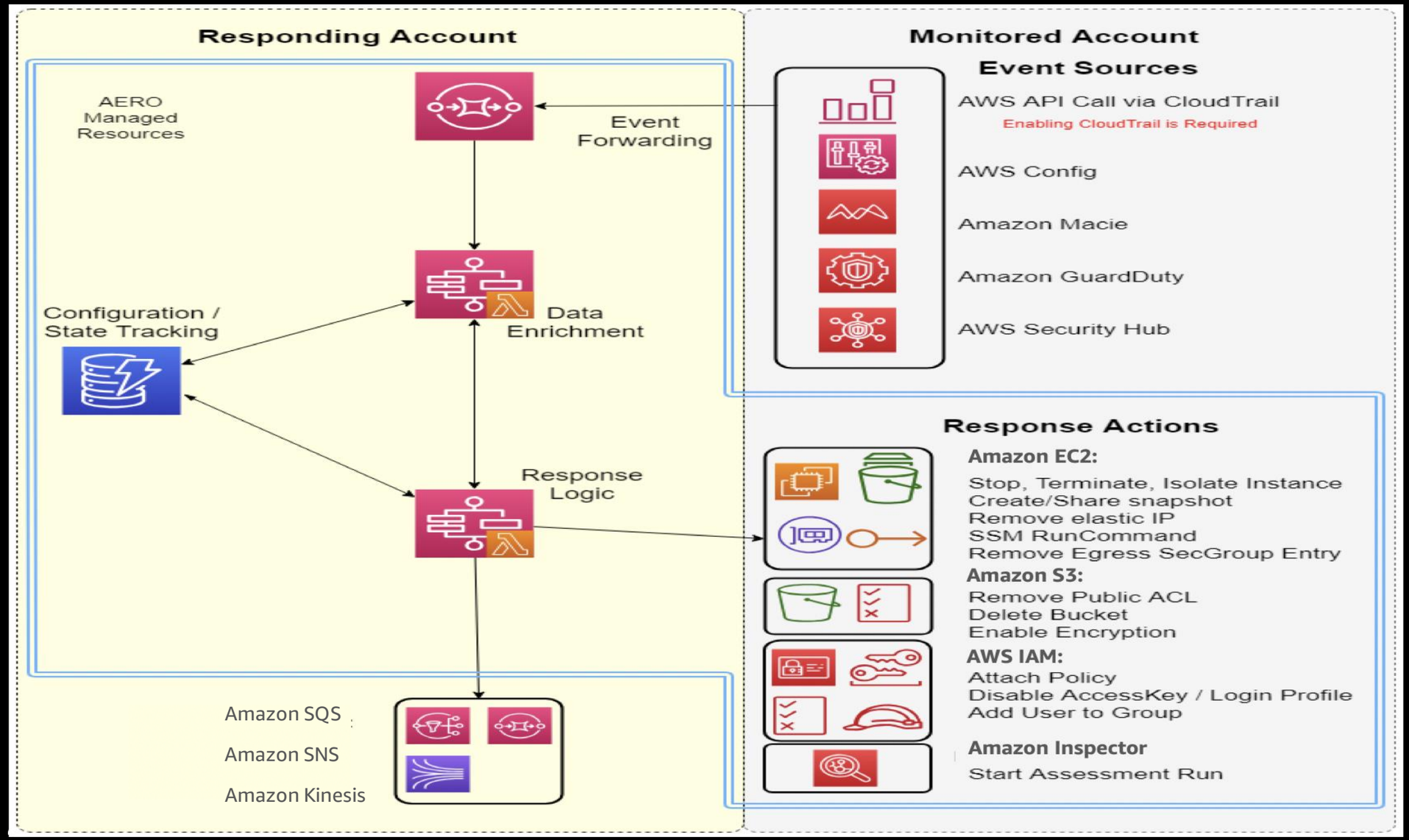
AWS 中国（宁夏）区域由西云数据运营
AWS 中国（北京）区域由光环新网运营

初始上云阶段安全最佳实践(必备安全组件)



AWS 中国（宁夏）区域由西云数据运营
AWS 中国（北京）区域由光环新网运营

业务增长阶段安全最佳实践（自动化响应）



业务平稳阶段安全最佳实践(大数据安全)

业务系统

AWS IAM
Amazon RDS
Amazon EC2

全局流数据

Amazon Kinesis
AWS CloudTrail
Amazon S3
AWS Lambda

大数据分析

Amazon EMR
Amazon Redshift

客户网络

AWS CloudFormation
VPC
Amazon WorkSpace

某些客户在 AWS 中创建了流数据洞察管道，并由 Amazon Kinesis 管理的大数据处理服务处理实时交换分析。 客户还将见解管道与 AWS CloudTrail 日志文件集成在一起，这些日志文件发送到 Amazon Simple Storage Service（Amazon S3）存储桶，通过 Amazon EMR 和 Amazon RedShift 进行大数据分析。 这为客户提供了整个 IT 环境的完整，透明和索引化的审计日志，及时发现异常网络行为和风险。

感谢参加 AWS INNOVATE 2020 在线技术大会

我们希望您在这里找到感兴趣的内容！

也请帮助我们完成**投票打分**和**反馈问卷**。

欲获取关于 AWS 的更多信息和技术内容，可以通过以下方式找到我们：

- 微信订阅号：AWS 云计算（awschina）
- 微信服务号：AWS Builder 俱乐部（amazonaws）
- 新浪微博：https://www.weibo.com/amazonaws/
- 抖音：亚马逊云计算（抖音号：266052872）
- 视频中心：http://aws.amazon.bokecc.com/
- 博客：https://aws.amazon.com/cn/blogs/china/
- 更多线上活动 ： https://aws.amazon.com/cn/about-aws/events/webinar/

AWS 中国账户注册

AWS 全球账户注册

AWS INNOVATE ONLINE CONFERENCE

AWS 中国（宁夏）区域由西云数据运营
AWS 中国（北京）区域由光环新网运营