亚马逊云科技

GSI 全球行

云上护航 安全同行

安全合规解决方案

云上创新 共赢全球

亚马逊云科技

扫码下载解决方案

数据智能解决方案

汽车行业解决方案

生命科学解决方案

安全合规解决方案

SAP 解决方案

可持续发展解决方案

通用解决方案

目录

埃森哲Security Landing Zone（安全着陆区）服务解决方案

应用场景

企业需要在云上建立安全着陆区(Security Landing Zone)，以构建一个安全合规的、可以充分信任的、能满足各种业务要求的云环境：

> 企业需要一个合规并符合企业自身安全需求的云基础环境。

> 为用户提供一个安全可信的云环境基础以放心地进行系统迁移和应用开发。

> 跨国企业潜在待迁移系统复杂。

埃森哲在中国和全球具有多年的数字化转型咨询和交付经验，与亚马逊云科技(Amazon Web Services)有着紧密的合作，帮助加速亚马逊云科技中国区的用户构建安全可信的、满足法律法规以及企业合规要求并适用于不同部门的、灵活可扩展的亚马逊云科技云上着陆区。

痛点和需求

上云是企业数字化转型的趋势，同时也对企业的 IT 建设和管理提出了新的挑战。如何构建一个安全合规的云上信息系统环境，能支持企业中不同用户的快速增长并且互不干扰、资源访问可控、成本可控，与本地数据中心安全网络连接，并且能满足审计需要，同时需要以较低的管理成本来达成管理要求，这些通常都是我们企业的 IT 管理部门需要考虑的。

- 所处行业和国家有特殊合规要求（LOB / IT）
- 快速增长企业不同部门用户有各自独立工作环境的需要（IT / InfoSec）
- 合适的权限控制并满足追溯和审计要求（IT / InfoSec）

常见问题和切入点

> 一些相关的典型的客户常见问题如下：

- 云上的账户该怎么组织分配?
- 云上网络该如何构建才能满足安全需求?
- 如何集中管理权限和日志以备审计需要?

方案价值和客户收益

本方案利用了埃森哲在咨询和交付领域的专业能力和亚马逊云科技在公有云领域的技术先进性，结合产品功能和最佳实践：

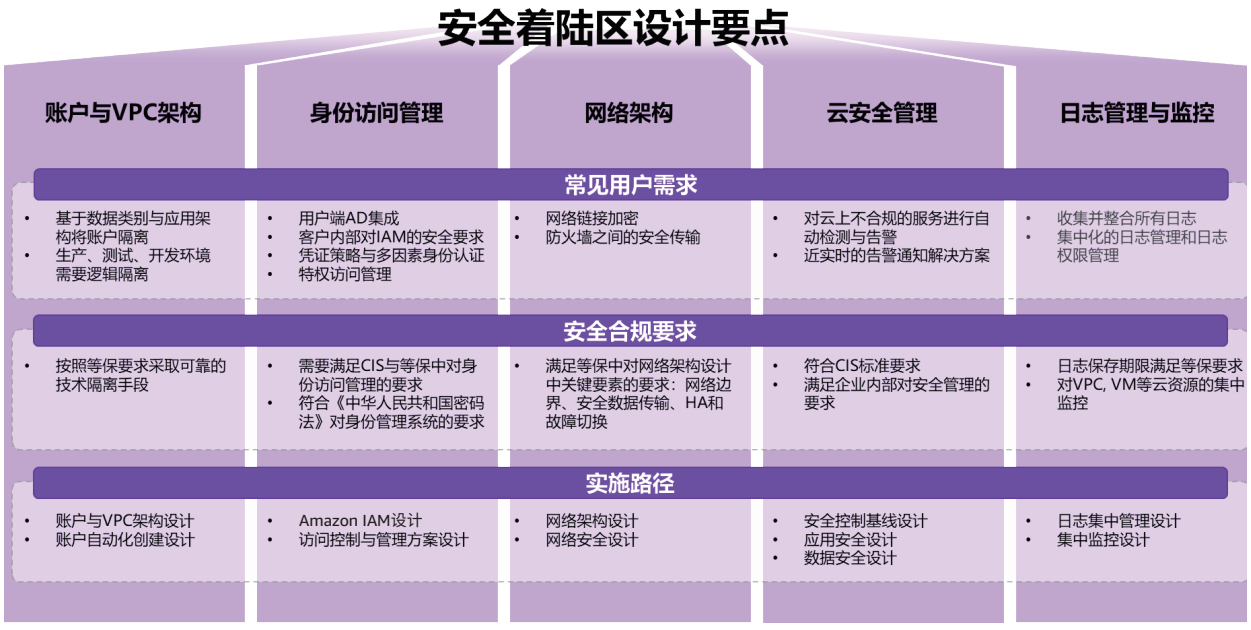
基于亚马逊云科技和埃森哲最佳实践，为用户提供一个安全的可配置的企业级的云资源环境，满足合规需求。

基于用户规模，方便可扩展。为后续的云迁移和应用开发奠定基础，加速数字化进程。

基于埃森哲各行业咨询和交付项目中的丰富经验，充分理解不同行业、地域对安全着陆区的具体需求。

方案介绍

埃森哲基于行业理解和安全合规的实践经验，采用以安全合规需求为驱动的设计思路，从企业所在行业、地区以及企业自身的信息安全策略出发，设计出满足特定合规要求的安全着陆区。例如对于中国区的企业用户而言，满足网安法和等保 2.0 是其非常重要的考量要素。



图示1:安全着陆区设计要点(© 2022 埃森哲版权所有)

成功案例

埃森哲为某全球知名生命科学企业设计了安全着陆区，在亚马逊云科技的中国区域，一些服务由于安全法规的要求和 Global 区域有所不同，并且有一些服务落地时间有滞后，因此不能使用 Global 区域提供的安全着陆区解决方案，在整体方案设计时需要考虑到中国区域的特点，对客户所需的暂时缺失的亚马逊云科技中国区服务，考虑合适的满足中国法律法规要求的亚马逊云科技合作伙伴替代产品。

该安全着陆区在账户设计、网络连接、安全防护等方面均符合中国法律法规要求，以及该公司内部安全管理规范：

- 采用多账号管理策略满足企业多组织管理需要；
- 采用 IAM Federation 方案进行联合身份认证和特权访问的管理；
- 连接亚马逊云科技中国区及海外云环境和本地数据中心的安全的网络设计；
- 集中日志管理、配置规则的管理，以及证书和密钥的管理等等。

亚马逊云科技相关服务

和本方案相关的亚马逊云科技主要服务如下：

埃森哲数据出境安全解决方案

应用场景

在全球数字化经济的大背景下，中国相继出台了一系列法律法规来规范数据的跨境流动。不论是在华的跨国企业，还是出海的中国企业，业务活动中都不可避免地会涉及到数据的跨境传输，需要积极应对监管，满足数据出境的合规要求。

痛点和需求

数据发现与分类难

随着云计算、移动互联、大数据、物联网等技术的普及，企业在业务发展过程中产生了海量的数据，类型复杂，存储分布于云上、云下，给数据的发现和分类带来了很大的挑战。

数据流梳理和风险识别难

随着数字化的推进，企业会应用大量的信息系统，不同系统之间存在大量的数据流转，数据流转路径的梳理也成为应对数据出境合规的难点之一。 此外，企业对于潜在的数据跨境流转缺少完善的风险识别方法和风险量化标准。

持续合规和技术落地难

数据出境合规是一个长期且持续的监控、评估和不断优化的过程，企业需要长期投入来不断完善数据出境安全。安全保障技术能力的建设也是数据出境合规工作中的重点，如何选择合适的安全技术工具并制定合理的运营流程，在满足合规要求和方便业务开展之间寻求平衡也是企业在完善数据出境安全技术保障措施时需要重点考虑的因素。

常见问题和切入点

- 如何识别和梳理数据出境安全规制的数据？
- 如何确定数据出境安全的合规路径？
- 如何实施数据出境安全相关评估工作并针对发现的问题进行整改？
- 如何和第三方（如云服务提供商、数据受托处理方等）约定数据出境安全的责任和义务？

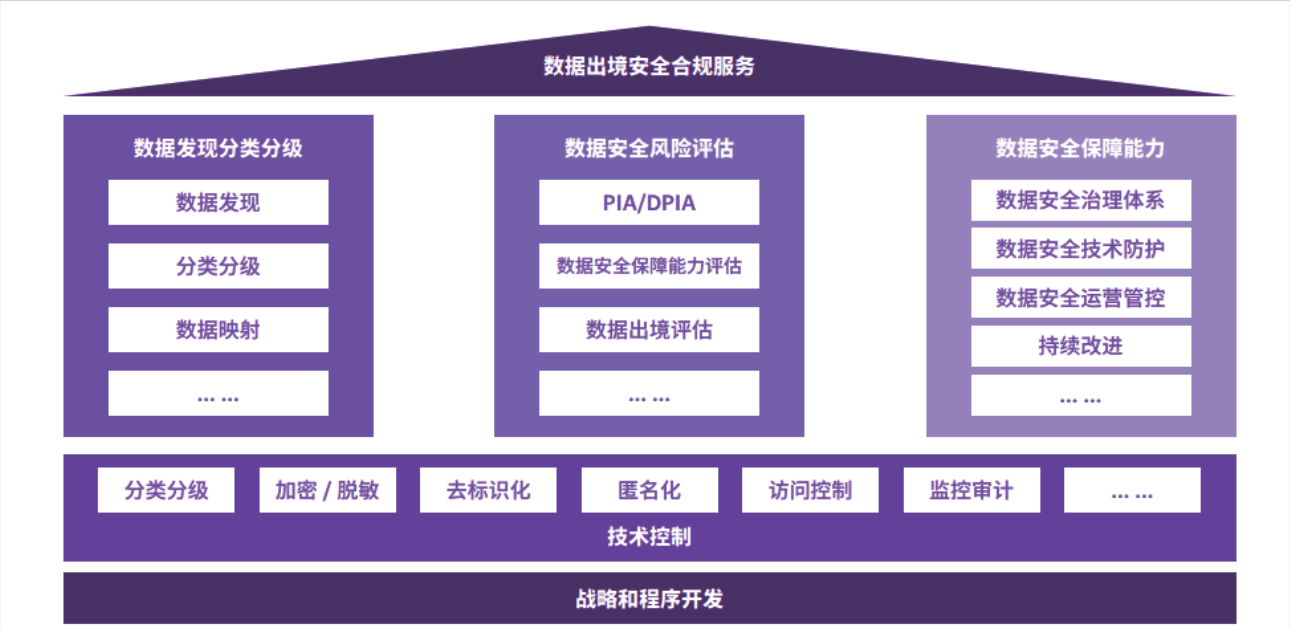
方案价值和客户收益

埃森哲针对数据出境安全合规提供从数据梳理、数据出境风险评估，到平台工具的落地实施与持续运营的服务，帮助客户实现长期可持续的数据出境安全合规。

同时，埃森哲基于丰富的行业战略咨询经验与解决方案落地及运营能力，为客户提供从数据安全治理体系规划咨询、数据安全技术能力落地实施、数据安全能力评估及数据安全运营服务，包括数据出境场景下典型应用的整改方案及落地实施，如云安全设计、云迁移、Salesforce 本地化、Workday 敏感信息拆分、SAP 迁移等，不仅帮助客户满足数据安全合规要求，同时帮助客户构建并提升整体数据安全保障能力。

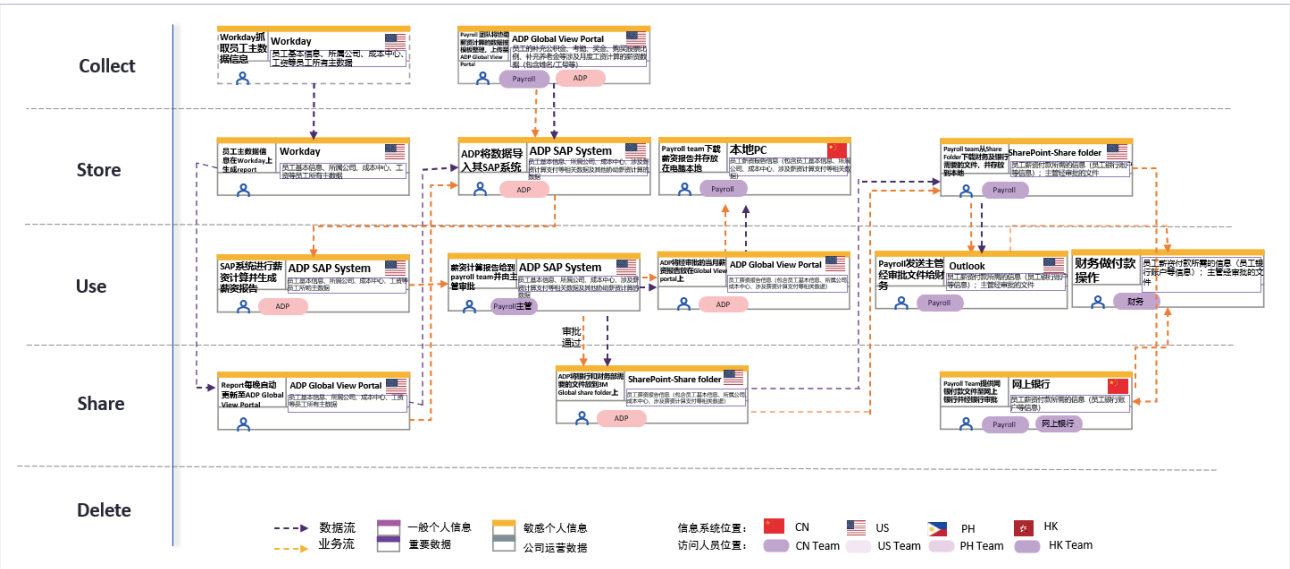
方案介绍

埃森哲埃森哲基于自有的、成熟的数据保护框架，结合市场领先的平台与工具，通过集成数据源自动扫描、模型匹配、数据统计、机器学习与智能分析等技术，完成数据发现、数据意义识别、业务类型确认、数据分类、数据清单建立与数据映射等工作，为数据出境安全合规提供评估、持续改进和运维的基础。在此基础上，依据数据出境安全评估办法及相关国家标准，对企业的数据出境安全管理能力和技术能力进行评估，识别潜在的风险，并结合企业实际情况提出切实可行的整改建议。评估内容包括管理组织体系和制度建设情况，全流程管理、 分类分级、应急处置、风险评估、个人信息权益保护等制度及落实情况，以及在数据收集、存储、 使用、加工、传输、提供、公开、删除等全流程所采取的安全技术措施等。同时，结合自身在数据安全咨询、技术能力整合和安全落地运营的端到端交付能力的经验和优势，帮助客户完成整改方案的实施和落地。



成功案例

埃森哲为某全球知名生产制造企业进行了数据出境评估和申报工作，客户业务流程复杂，应用繁多，数据量非常大，而且各种应用系统与 global 联系紧密，涉及数据出境的场景众多。埃森哲基于成熟的方法论和丰富的经验，通过深入理解客户的业务活动、IT 架构以及系统和应用，帮助客户梳理复杂业务和组织架构中的数据，形成数据清单和数据流图，识别涉及出境的业务场景、系统和数据，并对其展开全面的数据出境安全风险评估。针对评估中识别出的差距和风险，结合客户实际情况，提出切实可行的整改建议，帮助客户降低数据出境的风险，满足数据出境的合规要求，进而减少潜在的因不合规造成的业务中断的可能性。



Atos SOC as a Service解决方案

应用场景

SOC 安全运营中心一站式建设与运营。

缺乏 SOC 安全运营，或者希望提高 SOC 运营的 ROI。

希望获取到业界知名的 SOC 安全运营服务。

痛点与需求

随着用户业务数字化的不断演进，IT 设施往往部署在各类公有云、私有云、IDC、边缘节点以及用户本地环境中，基础设施与应用架构的复杂与多样，不断变化的安全与威胁、严格的合规要求为用户在 SOC 建设、运营等带来全新的挑战；传统 SOC 的交付与运营模式往往意味着低效的交付过程与高昂的维护成本，基于亚马逊云科技的 Atos SOC as a Service 解决方案可以有效的帮助客户解决安全运营与合规等方面的痛点问题：

- 多云、混合云等复杂场景下的 SOC 建设和运营
- 传统 SOC 复杂的建设与运营流程和高昂的花费
- 国内外日趋严格的法律法规带来的安全合规要求
- 业务快速迭代引发的 DevOps 所带来的安全挑战
- 缺乏长期的、高质量的、可持续的 SOC 运营服务
- 企业安全运营专业人士短缺

适用行业

制造　汽车　医药　能源　消费品

公共服务　媒体　……

方案价值

1 一站式安全 SOC 交付与运营能力

Atos SOC as Service 能够最大程度简化企业用户在建设与运营 SOC 过程中所涉及的集成、实施、服务等，通过与亚马逊云科技合作伙伴合作，通过统一平台入口获得全局的安全事件告警、威胁分析、风险分析、漏洞管理、用户行为分析等安全能力；结合 Atos 多年在全球 SOC 运营所积累的经验，为企业用户提供一站式、端到端的 SOC 安全交付与监控服务能力。

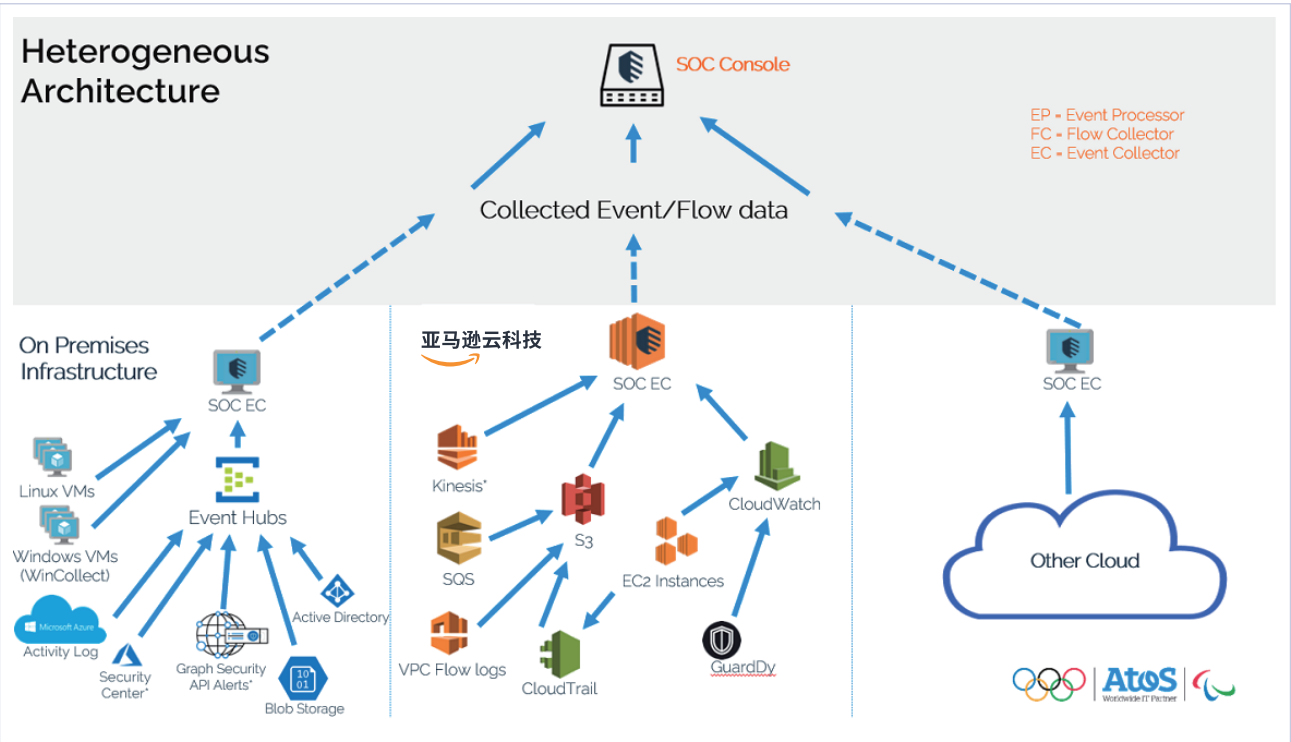
2 安全投入成本的节约和持续优化

Atos SOC as Service 能够为用户提供快速交付、按需订阅的 SOC 运营与服务能力。用户可根据具体需求灵活订阅服务，一站式接 入Atos SOC 云平台，有效节约在安全运营与服务方面的投入。

3 成熟的 SOC 建设框架与丰富的 SOC 运营经验

Atos 在全球拥有 15 个 SOC 运营中心，6000+ 安全专家，多次为奥运会等全球大侠赛事提供 SOC 安全运营与服务，积累了大量应急响应、事件分析等经验，在关键业务的安全运营与服务等方面能够为用户提供长期的、高质量的、专业的保障。

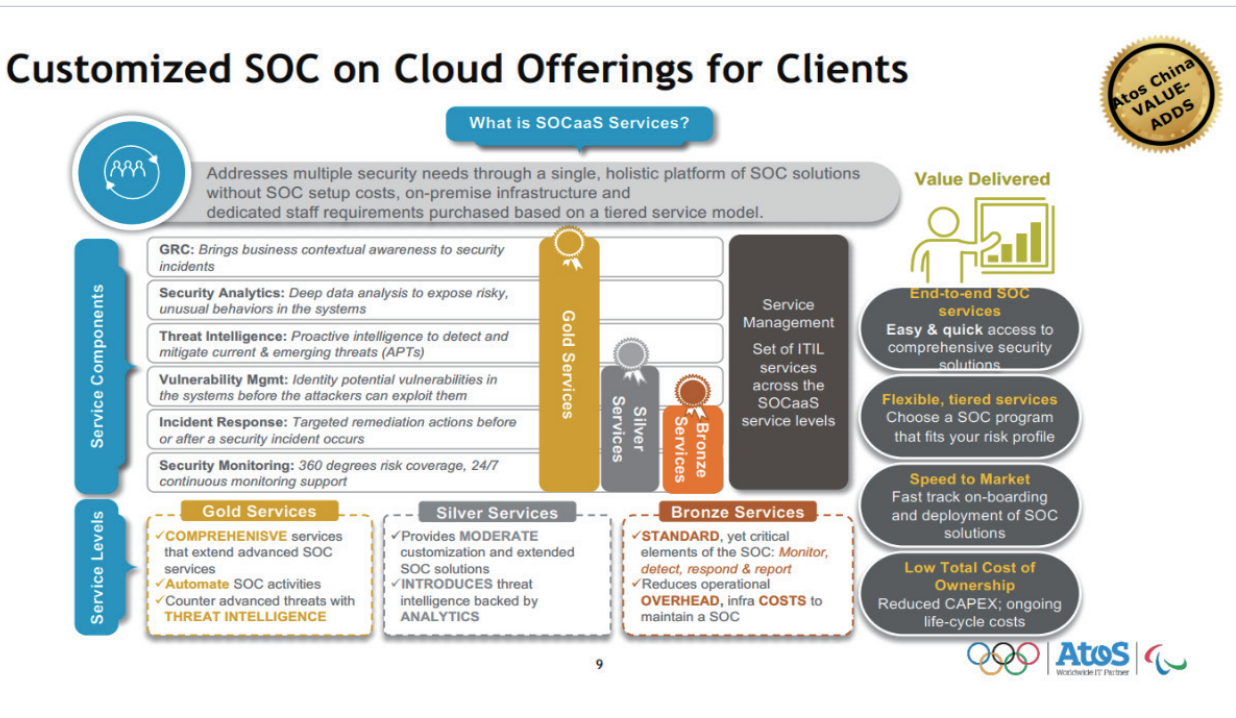
方案介绍



1. SOC 软件平台底层资源部署在亚马逊云科技的计算和网络等服务中，通过云平台多可用区以及多租户、多副本等安全能力保证基础资源的稳定运行和快速访问。

2. 用户采购或订阅 SOC 服务后，无需另外采购硬件和软件产品，可以快速将用户多云和混合云环境中相关 IT 系统、网络与安全设备、应用等产生的日志、网络流等数据通过安装采集器组件或者采用标准协议的方式实时发送至 Atos SOC 平台。Atos SOC 平台为客户建立单独隔离的日志分析区，通过上下文关联、AI 等对用户的日志和事件数据进行多维度建模分析，识别安全威胁和安全风险。同时联合 Atos 平台提供的安全运营服务，可以显著提升用户在安全监控响应、威胁分析、安全合规、风险控制等集中管控能力。

3. 安全运营服务作为 SOC 重要的组成部分，安全事件的响应、分析以及处理效率，安全人员的及时响应和业务专业性等对用户关键业务的安全稳定运行有着至关重要的作用。Atos SOC 服务可通过本地或者远程的方式为用户提供覆盖全年 7x24 的安全运营服务，服务涉及安全事件响应与威胁检测，安全事件分析与溯源取证，漏洞管理以及自动化编排等，为用户关键业务的长期稳定运行保驾护航，同时满足监管合规的需求。



服务交付方式

订阅模式：

根据使用场景和需求不一样，客户可以通过 Amazon Marketplace 订阅或者与 Atos 直接签订合同购买该服务。Atos 将根据客户 IT 资产规模以及所选择的 SLA 等级不一样提供不同的服务价位选择。

目前 Atos SOC on Cloud 提供三种不同等级的服务：

铜牌服务：

标准的安全运营 SOC 服务方式，主要包含了 7x24 小时持续的安全监控和响应服务，包括监控、发现、响应和报告服务。

银牌服务：

在铜牌服务的基础上，增加漏洞管理服务，定期进行潜在漏洞扫描和发现，在攻击者利用之前报告这些漏洞。

金牌服务：

在银牌服务的基础上增加：

- 威胁情报管理-通过全球威胁情报库及时发现常规和非常规的安全威胁
- 智能应对-采用 AI 和 SOAR 等自动化编排对常规威胁进行自动快速响应
- 安全分析-安全专家对非常规安全威胁进行深度分析、及时响应和处理

Atos 将提供专业的安全团队根据客户订阅的 SLA 协议提供相应的服务，Atos 的 SOC 运营团队主要分为安全监控团队和应急响应团队。安全监控团队对客户接入 SOC 平台的系统和日志提供 7X24 小时的不间断监控，而应急响应团队则会对监控发现的安全威胁进行分析处理和及时响应。此外，Atos 全球 SOC 团队将对 SOC on Cloud 平台进行持续优化和升级。

亚马逊云科技相关服务

Amazon EC2 | Amazon S3 | Amazon GuardDuty | Amazon CloudTrail

Amazon CloudWatch | Flow logs | Amazon SQS

CI&T基于亚马逊云科技的Drupal托管解决方案

Drupal 是一款开源的内容管理系统，有很多世界 500 强公司和中国企业都在使用它，但是，在中国市场上却很难找到一套成熟且符合中大型企业需求的 Drupal 托管解决方案。为此，我们自主研发了具备完整基础架构的 Drupal 应用程序生命周期管理套件，以支持从开发、测试到生产的整个 Drupal 部署以及稳定运行的工作流程。

行业痛点分析

虽然有需求，但企业内部的开发团队往往不具备足够的技能与时间去创建及维护一套高可用、自动化的 Drupel 托管解决方案。

全面满足企业用户需求

- Drupal 站点或站群管理及开发
- 云服务架构的管理
- 高可用及安全配置
- 适用于 Drupal 的自动化备份及监控方案
- 持续部署方案

方案实现方式

全面自动化

基础架构

自动化创建方案所需的云服务，以及必要的第三方软件包

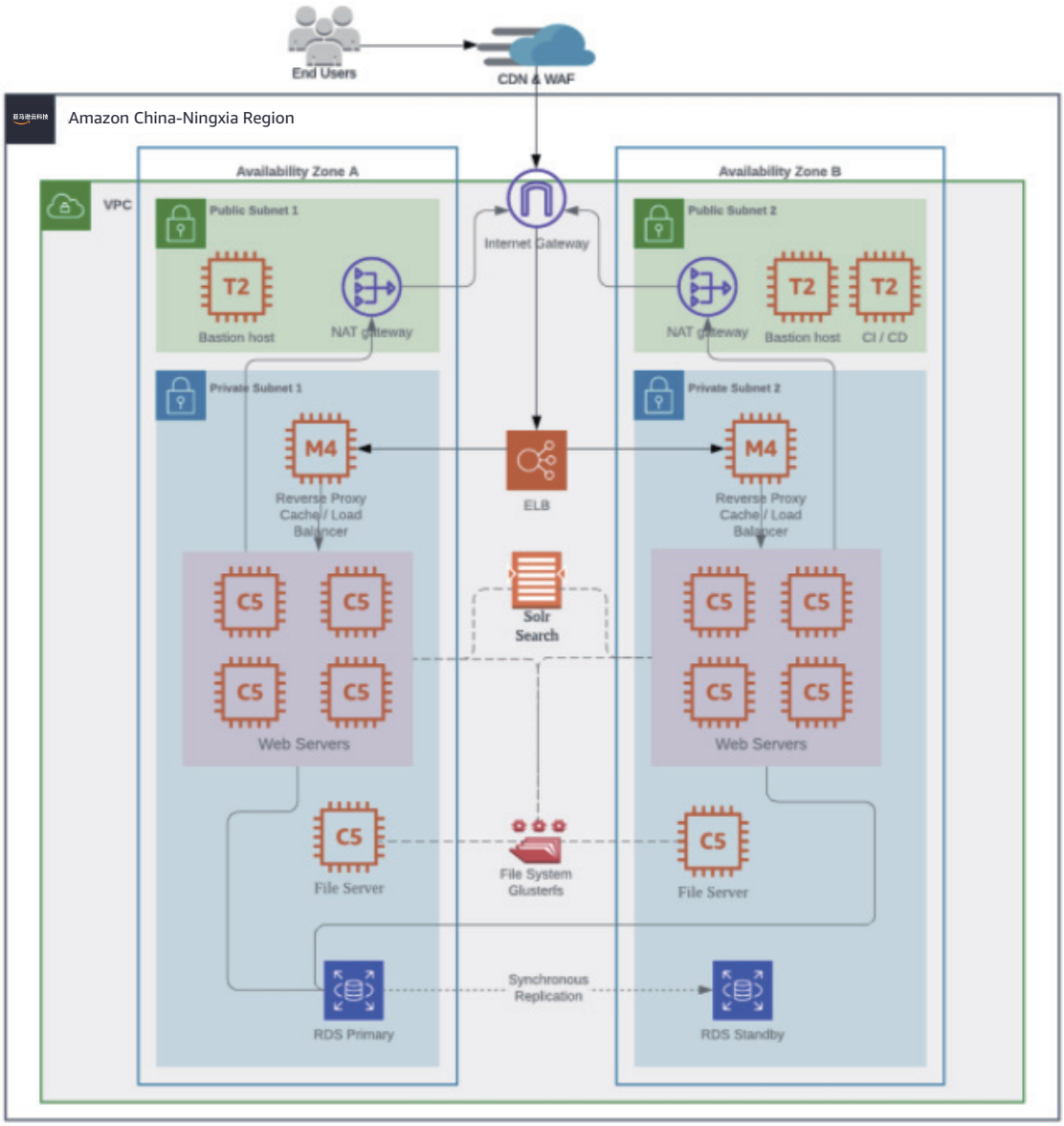
部署

自动化部署及回滚机制

备份

灵活的自动化备份策略以及多区备份同步机制

基于亚马逊云科技的架构



适用行业

零售业　医药　制造　航运　教育　其他

功能概述

基础架构自动化

Drupal 站点所需的服务器、数据库、文件备份等等服务全自动化搭建。

可持续部署 Pipeline

基于 Jenkins 的自动化运维，可视化的部署以及回滚流程。

集中化日志管理

Nginx、Apache、PHP、Drupal 等服务日志集中化管理。

完善的监控机制

从服务器、数据库、Drupal 应用、SSL 等等全方位的监控，让您深入了解各个服务的运行状况。

完善备份机制

自动化备份机制可保证数据的安全，从而极大程度的减少了遭受攻击或者人为失误操作带来的影响。

服务可扩展性高

提供具有高可用性的完全托管，可扩展的多服务器服务，完美支持热加载，无需停止任何服务。

完善的权限管理机制

为开发人员提供操作服务器和数据库的最低权限，避免开发人员误操作导致系统或数据库崩溃。

关键价值

安全合规

基于亚马逊云科技(Amazon Web Services) 安全的基础服务架构，我们还提供其他层面的安全合规措施，比如符合中国等保 2.0 要求的安全产品、权限控制管理、日志审计等等。

为 Drupal 量身打造

完美支持 Drupal 多站点部署，以及多域名、数据库的关联，支持 Memcache，Varnish 等 Drupal 常用缓存技术。

高性能与高可用

提供高可用、高性能且易于扩展的 Drupal 运行平台，确保服务连续稳定运行。

方案应用场景

提供基于 Drupal 的高可用、高性能、连续稳定的额安全运行环境，高效的自动化运维工具、流程以及服务监控。

DXC SIEM/SOC解决方案

公司概述

DXC 在 70 多个国家/地区拥有 4000 多名经过云认证的专业人员，作为亚马逊云科技解决方案提供商和高级咨询合作伙伴，每年将超过 27,000 个工作负载转换和管理到云上，确保我们的客户在云之旅中取得成功。我们帮助您确定云上的工作负载，转换应用程序并管理迁移，以最大限度地降低风险和成本。DXC 提供全方位的亚马逊云科技服务交付能力，以我们深厚的技术知识、经验，向客户提供卓越的亚马逊云科技服务。DXC 专家、流程和服务可确保您的云环境风险降低、安全性、法规合规性和完整的运营治理。DXC 依据自身的全方位的服务能力，为客户在亚马逊云科技上提供技术解决方案和流程组合支持，以持续监控和改进组织的安全架构，同时预防、检测、分析和应对突发网络安全事件，降低客户云上资产的风险，并保护的客户云上投资。

痛点和需求

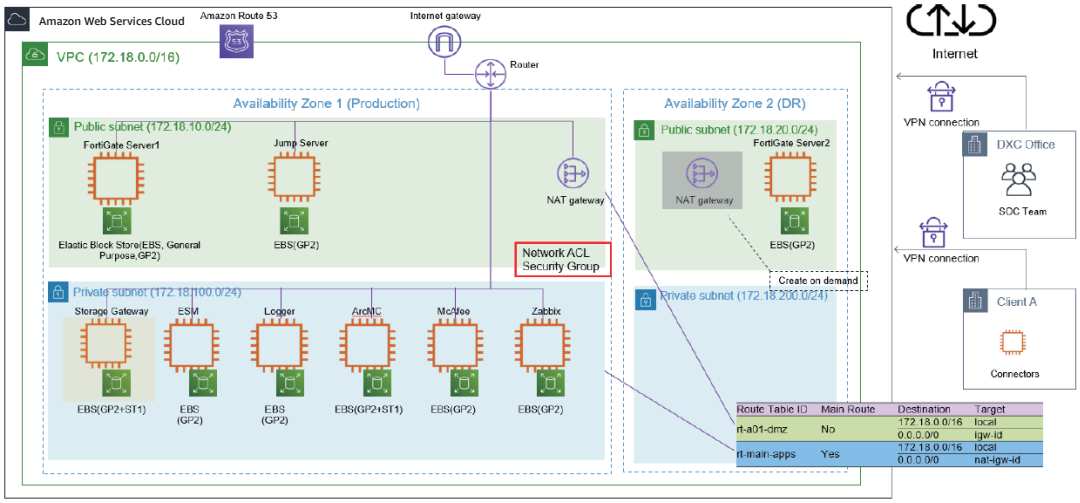
随着越来越多的工作负载和应用程序迁移及部署到亚马逊云科技，客户需要对云上资产和业务的连续性进行不间断的持续监控，同时需要满足中国对于信息安全的法律法规，DXC SOC（Security Operations Center）解决方案可以有效的帮助客户解决以下痛点：

- SOC 的设计必须与全球服务部门保持一致，并符合中国的当地监管的要求
- SIEM 系统需要管理和监视数量巨大且类型多样的设备和日志源
- 客户的 IT 环境非常复杂，是混合云架构
- 系统架构文档分散且混乱，需要分析大量设备和应用的具体情况
- 项目实施周期非常紧张
- 网络架构复杂，现有的产品很难实现，而这是项目所必需的
- 考虑成本和性能，如何采用合适的安全体系

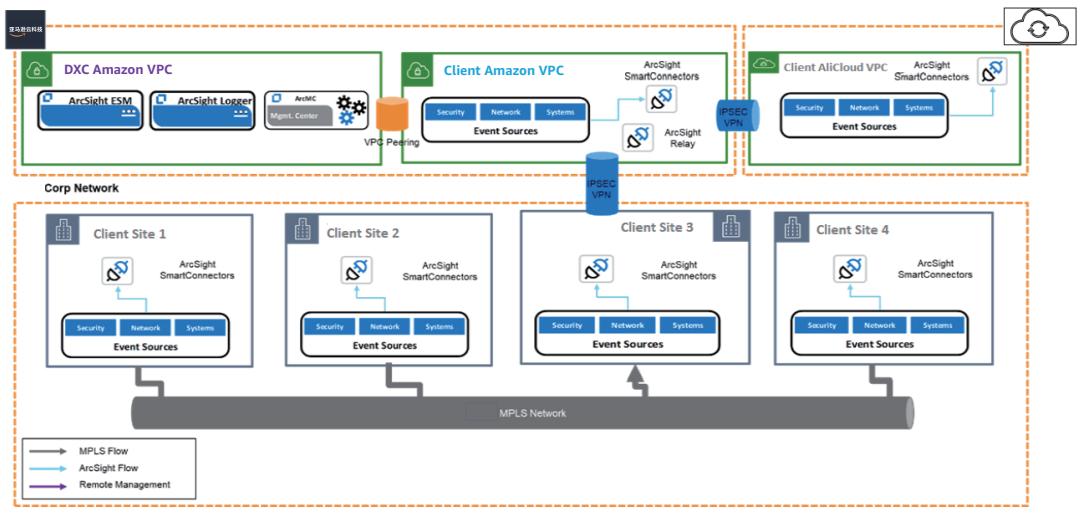
方案实现方式

SOC 设计

DXC Security SOC EDR Architecture on Amazon Web Services



DXC Security SOC SIEM Architecture on Amazon Web Services



设计与咨询

- 完整的沟通和详细的现场调查以确定架构设计
- 咨询服务，包括架构设计，迁移评估等
- 协助客户选择云以及和合适的技术

解决方案交付

- 基于中国的云设计的 SOC
- 遵循 DXC 的最佳实践，如监控时间和标准，安全事件响应时步骤措施，与第三方的合作

适用行业

汽车	机械制造	消费品	建筑	化工
石油	天然气和能源	公共服务	媒体	……

给客户带来的价值

- 实时监控和分析事件，以及出于合规或审计目的跟踪和记录安全数据
- 识别和检测潜在的安全威胁和漏洞
- 调查和应对网络威胁
- 组织安全管理
- 保护客户云上业务

应用场景

企业初次上云	满足已上云企业的合规要求

Deloitte.

德勤中国企业出海合规咨询解决方案

应用场景

中国企业出海需要满足海外不同地域法律法规要求，例如欧盟的 GDPR - 欧洲通用数据保护条例和北美的 CCPA - 加州消费者隐私法等。

> 业务扩张有出海需求，面临复杂的海外合规要求。

> 所属行业监管/合规要求严格，例如：金融、汽车、跨境电商、高科技、医疗健康等。

德勤帮助客户解读相应的法律法规，分析面临的问题和挑战，并提出应对策略以建立相应管理体系和构建数据安全技术平台，从而建立有效的数据安全合规保障体系。

痛点和需求

数字化经济下，数据资产成为企业最核心竞争力的来源，全球各国都在不断通过各种立法来规范数字化经济的发展。对于中国企业出海来说，面临的是双向合规的强监管时代，在某些场景下，网络安全合规甚至是比业务先行更重要的决定性议题。客户往往需要一个更加理性和有规划的过程，并从组织和技术等各个方面应对以下挑战：

- 业务部门不了解海外法规（LOB / Legal）
- IT 部门对相应系统改造和建设缺乏合规指导路线（IT / InfoSec）
- 执行部门需要权威第三方策略背书（IT / InfoSec）

常见问题和切入点

> 一些相关的典型的客户常见问题如下：

- 如何快速满足 GDPR 的要求？
- 数据跨境传输需要注意哪些事项？
- 已经经过身份识别取消的数据还是 PII 吗？

方案价值和客户收益

通过德勤为中国企业为提供出海合规咨询服务，可以：

为客户规避法律风险，让客户专注核心业务，解决合规担忧。

以安全为入口影响客户决策，展现亚马逊云科技优势并为后续新系统建设或迁移奠定基础。

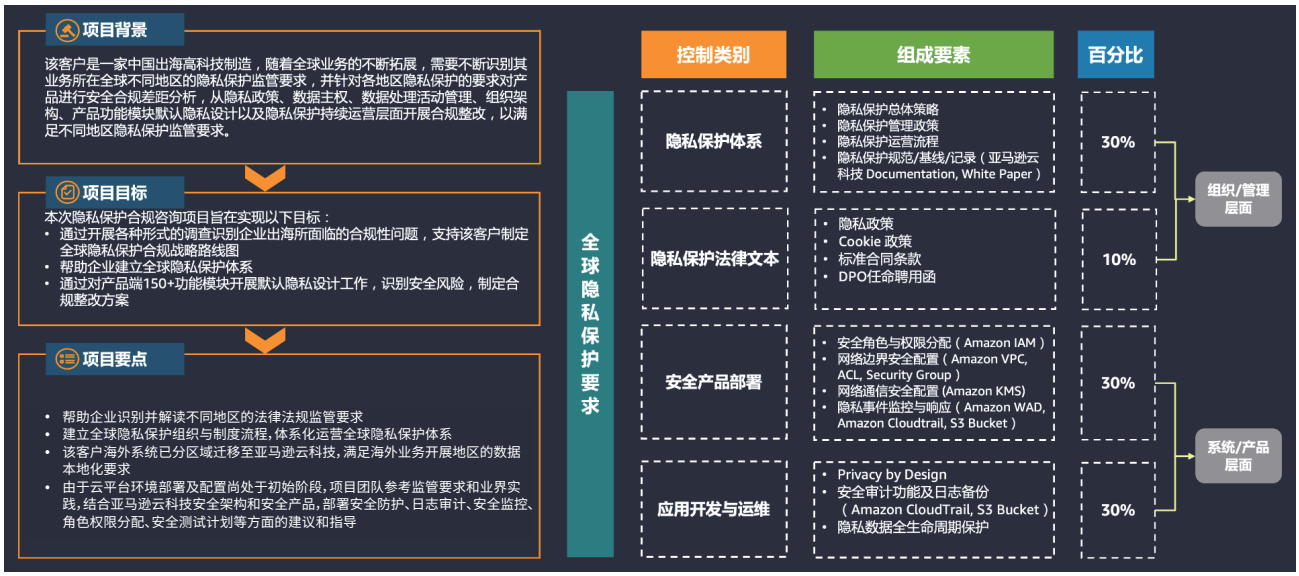
德勤业务覆盖全球，有从咨询到落地的一站式能力，充分保障从咨询到落地一致性。

方案介绍

在基于对国际法律法规解读的基础上，在个人信息或行业敏感信息安全治理方面，为客户提供最佳实践及架构设计的整体建议，从而建立有效的数据安全合规保障体系。（欧盟：GDPR - 欧洲通用数据保护条例；北美：CCPA -加州消费者隐私法）。

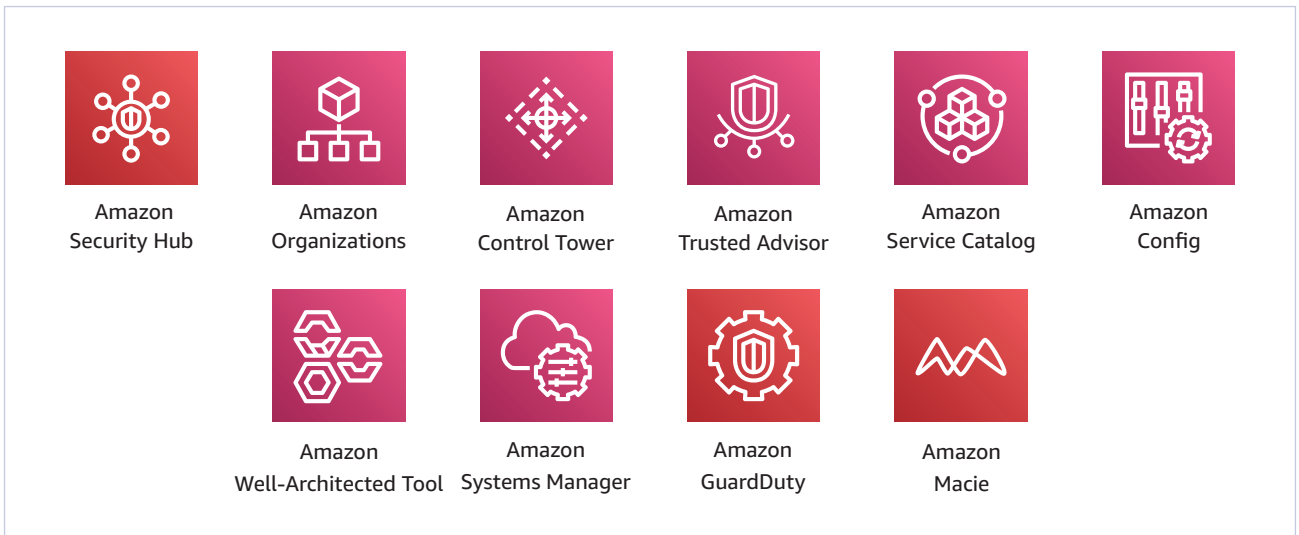
成功案例

德勤为某高科技制造企业出海隐私保护提供解决方案：



亚马逊云科技相关服务

安全合规是亚马逊云科技的首要任务，也是创新的根本保障。亚马逊云科技的技术架构保证了它可以为客户提供灵活、安全的云计算环境，因而成为企业出海的首选。和本方案相关的亚马逊云科技主要服务如下：



德勤跨国企业本土化合规咨询解决方案

应用场景

随着国内的《网安法》、《数安法》以及《个保法》相继出台，跨国公司在中国市场需要积极拥抱监管要求，实现主动合规。

> 客户在中国开展新业务，亟需本地合规建议。

> 客户现有外网系统尚未通过等保认证，面临国家监管风险。

德勤帮助客户解读相应的国内法律法规和行业监管要求，通过分析调查，发现差异，并提出应对策略以建立相应管理体系和技术平台，并最终帮助客户进行相关的测评和认证。

痛点和需求

我国数据安全管控的基本原则是要求重点行业（如汽车业、金融业、医疗健康业）的重要数据和达到一定规模的个人信息进行“本地化存储”。因此，“数据本地化”已经成为跨国互联网以及高科技公司在华开展业务所面临的挑战。企业在迁移业务系统到境内实现本地化的过程中，需要关注法律法规，确保本地化运行合规，同时加强数据安全保护，保障本地化系统的安全运行，从容应对以下挑战：

- 跨国公司对中国法律法规不熟悉（LOB / Legal）
- 等保认证要求客户多部门配合协调费时费力（IT / InfoSec）
- 执行部门需要权威第三方策略背书（IT / InfoSec）

常见问题和切入点

> 一些相关的典型的客户常见问题如下：

- 跨国企业如何在中国保证合规？
- 在中国系统是否需要进行 MLPS 2.0 认证？
- 美国员工可以访问在中国的系统吗？

方案价值和客户收益

通过德勤为跨国企业在中国开展业务提供合规咨询和等保认证等服务，可以：

为客户规避法律风险，让客户专注核心业务，解决合规担忧。

以本地法规咨询和等保要求为入口影响客户决策，展现亚马逊云科技优势并为后续新系统建设或迁移奠定基础。

德勤业务覆盖全球，有从咨询到落地的一站式能力，充分保障从咨询到落地一致性。

方案介绍

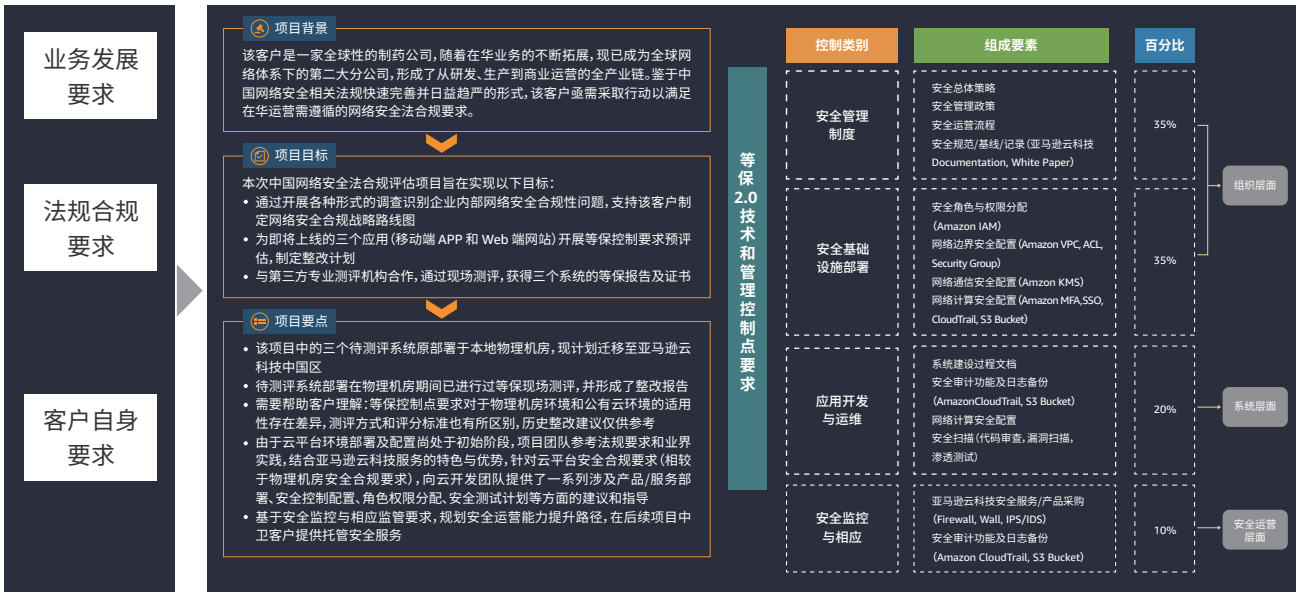
基于对等保制度、数据保护法、及行业监管要求的理解，为客户从管理和技术两个方面提供现状调查、差异分析、安全改善建议整体报告。

- 等保 1 级 适用于客户内网安全自查，无需认证；
- 等保 3 级 适用于存储大量个人信息的系统（如 CRM）或国家重点监督的系统（如工控系统/物联网/云平台等）；
- 等保 2 级 适用于非核心的客户外网系统，如企业官网；
- 等保 4 级、5 级 适用于关系国计民生的关键信息系统，一般与国家机关/国企有关，外企几乎不涉及。

德勤基于等级保护的咨询解决方案如下图所示：

成功案例

德勤为某全球性制药公司提供基于等保的咨询解决方案：



亚马逊云科技相关服务

和本方案相关的亚马逊云科技主要服务如下：

安全通信网络

- Amazon VPC
- Amazon CloudFront
- Amazon Direct Conncet
- Amazon API Gateway
- Amazon Elastic Load Balancing
- Amazon Route S3
- Amazon Cloud Map
- Amazon Certificate Manager
- Amazon CloudTrail

安全区域边界

- Amazon VPC
- Amazon WAF
- Amazon CloudTrail
- Flow logs
- Endpoints
- Network access control list

安全计算环境


Amazon IAM


Amazon Directory Service


Amazon Resource Access Manager


Amazon Certificate Manager


Amazon Secrets Manager


Amazon Key Management Service


Amazon CloudTrail


Amazon Lambda

安全管理中心


Amazon Security Hub


Amazon Systems Manager


Amazon Organizations


Amazon GuardDuty


Amazon Trusted Advison


Amazon Resource Access Manager


Amazon CloudWatch


Amazon CloudTrail

德勤制药行业云上计算机化系统验证（CSV）解决方案

应用场景

在生命科学行业进行数字化转型的过程中，云技术的应用极大地提高了企业服务的可扩展性和可靠性。然而，企业在上云时，需要保证其对制药行业 GxP 合规的遵从性。主要面临客户场景有：

客户新业务开展，系统未经过计算机化系统验证（CSV），面临合规风险。

客户想加速云计算的采用，但是对相应的 GxP 合规有疑虑。

德勤结合多年的海内外制药行业计算机化系统验证项目经验的积累，帮助企业在云上构建合规的生命科学应用，为药品生产企业提供从业务发展到技术框架方面的探讨和建议，为企业数字化转型提供催化剂。

痛点和需求

新版《中华人民共和国药品管理法》的颁布对药品生产企业在从事药品研制、生产、经营、使用和监督管理等方面提出了更高的要求。完备的计算机化系统建设不仅是企业信息化水平的体现，与质量管理息息相关，也是企业合规运营、长久发展的重要保证。对于全球化制药企业客户，GMP 是大家公认的行业质量控制的规范，对于国内客户，计算机化系统验证是大家都要遵守的监管要求：

客户对 GxP 和 CSV 合规要求不熟悉
（LOB / IT）

计算机化验证要求涉及内容广泛
（IT / InfoSec）

执行部门需要权威第三方策略背书
（IT / InfoSec）

常见问题和切入点

一些相关的典型的客户常见问题如下：

- 系统上云后对计算机化系统验证有什么影响？
- 计算机验证要做到什么程度才算足够？
- 哪些计算机系统需要验证？

方案价值和客户收益

德勤多年海内外制药行业计算机化系统验证为制药企业提供从业务发展到技术框架方面的建议，帮助企业进行数字化转型。

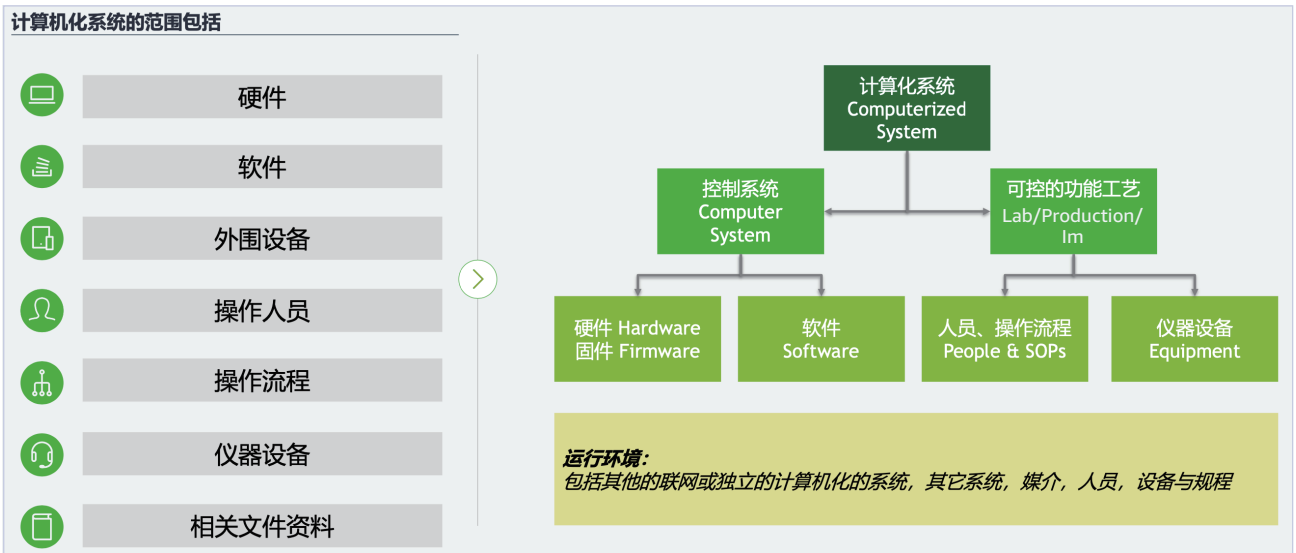
更好保证产品安全性和质量；更加可靠稳定的设备和系统；更稳定的产品质量持续性。

针对云上基础架构的搭建、验证和确认，并将其纳入到自身已有计算机化系统质量管理体系中。

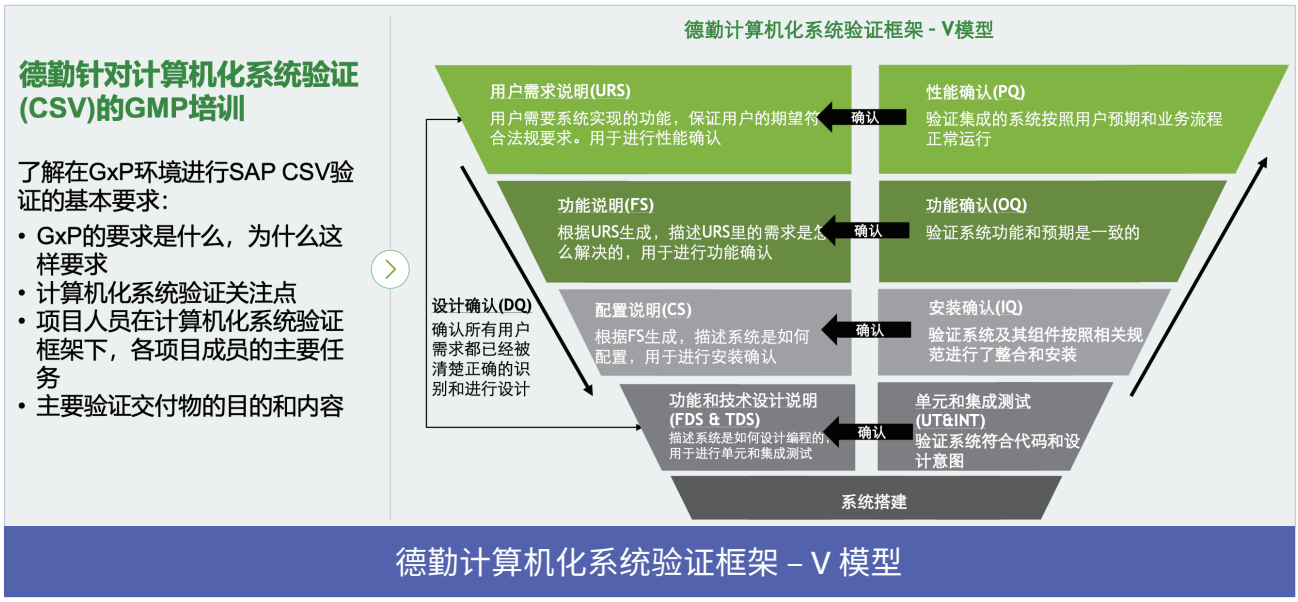
深刻理解 GxP 法规，准确把握各类系统的风险；体系咨询和 CSV 验证 一 站式服务。

方案介绍

在计算机化系统验证方面，德勤通过多年的海内外制药行业计算机化系统验证项目经验的积累和沉淀，形成了一套切实可行、适合当地行业特点的计算机化系统验证方法论。能够帮助客户验证系统，使其符合各项 GxP 法规和预定用途，产品能确保患者安全和质量要求，与产品质量有关的数据完整可信。计算机化系统的范围包括：硬件、软件、外围设备、操作人员、相关文件资料，如操作手册、SOP 等。



计算机化系统验证的范围



德勤计算机化系统验证框架 – V 模型

德勤的计算机化验证体系是弹性可伸缩的，可以根据客户质量管理要求，在现有流程和模版的基础上进行灵活调整，风险评估也会贯穿整个项目。我们建议在验证开始前，尽量明确未来可能的业务市场，从而考虑清楚 CSV 验证的语言。针对常规法规市场如中国、美国、欧盟等地区的 GxP 合规点，德勤可以根据自身的经验归纳总结出点对点的实施建议。

成功案例

德勤在与某国际化生物技术公司的 SAP 计算机化系统验证合作项目中，实施团队采用了高效、严谨、灵活的德勤计算机化系统验证方法论以确保计算机化系统合规，根据客户质量管理要求灵活调整细节方法，将风险评估贯穿整个项目的始终。对亚马逊云科技云上基础架构的搭建、运行和维护等根据法律法规进行充分的确认和验证。

亚马逊云科技相关服务

医药企业客户在将应用部署到亚马逊云科技云上后，通过云上的安全配置等，确保云上基础架构、云上服务和业务应用得到合理管控，以应对法律法规对云上计算机化的系统合规性、数据完整性的要求。和本方案相关的亚马逊云科技主要服务如下：

德勤安全运营中心及安全托管服务 (Managed Security Service) 解决方案

应用场景

全球化时代，信息安全威胁与挑战持续升级，安全事件频发，勒索软件愈演愈烈。云计算环境下，企业的信息安全管理的物理边界和责任边界更加泛化。

> 从传统机房模式转换为云模式，安全运营经验和人力不足，监控不完善。

> 企安全服务效率低下，安全态势难以有效可视化管控。

德勤通过云安全托管服务帮助客户加快在亚马逊云科技（Amazon Web Services）云上的旅程，为客户提供持续的安全保护和对必要资源的监控，帮助其加快创新和开发的速度。

痛点和需求

企业在推进数字化变革，不断通过技术革新来加速业务创新的过程中，不得不面临着各种安全运营的风险。然而，面对这些安全挑战，企业自身往往没有足够的经验，导致安全服务效率低下，安全态势难以有效可视化管控。

客户的业务有很高的安全运营要求
（LOB / IT）

客户对云上安全运营经验不足
（IT / InfoSec）

需要能够基于 SLA 提供安全服务
（IT / InfoSec）

常见问题和切入点

> 一些相关的典型的客户常见问题如下：

- 如何来保护大规模云工作负载？
- 希望更具成本效益的方式来保护云工作负载。
- 希望聚焦业务创新而不是解决运营安全问题。

方案价值和客户收益

结合德勤多年在安全运营上的经验，安全运营服务可以帮助客户：

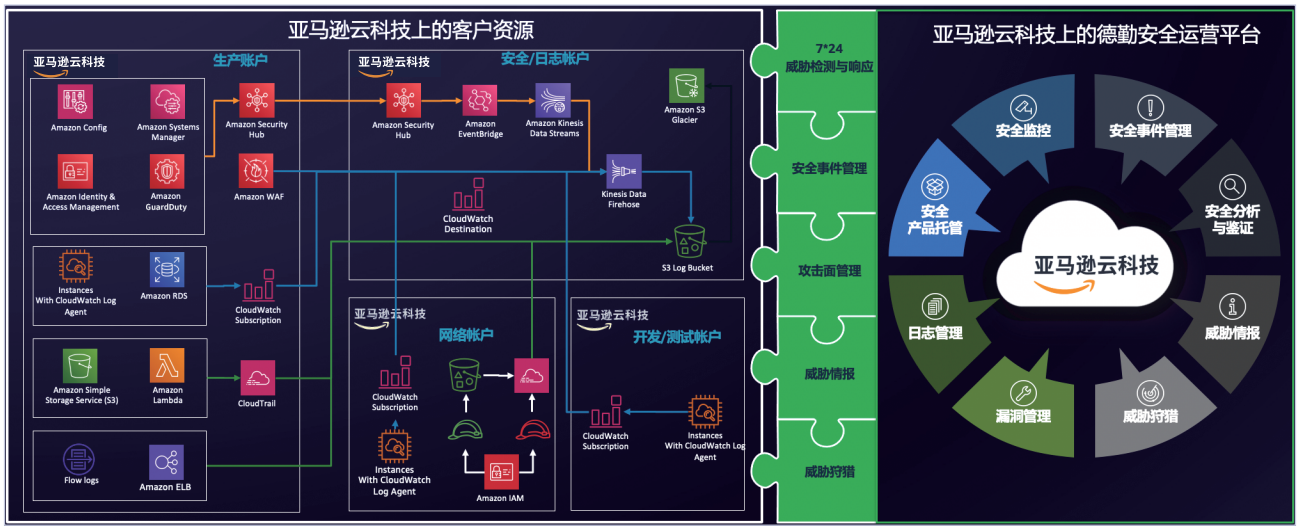
通过主动管理网络风险帮助组织变得更值得信赖、更有弹性和更安全。

提供量身定制的端到端的云安全服务，集成的安全工具和流程可提升响应速度，达到或超过行业标准。

经验丰富的安全工程师，对各行各业的安全解决方案有深入了解和良好交付记录。

方案介绍

中国的安全运营中心部署于亚马逊云科技中国区数据中心。双方共同定义了多样的可选服务包，并依此构建运营安全服务，以满足客户业务持续要求。通过将客户在云上和本地数据中心以及 SaaS 系统的安全信息汇总于安全运营中心进行威胁分析能够实现有效的安全监控。



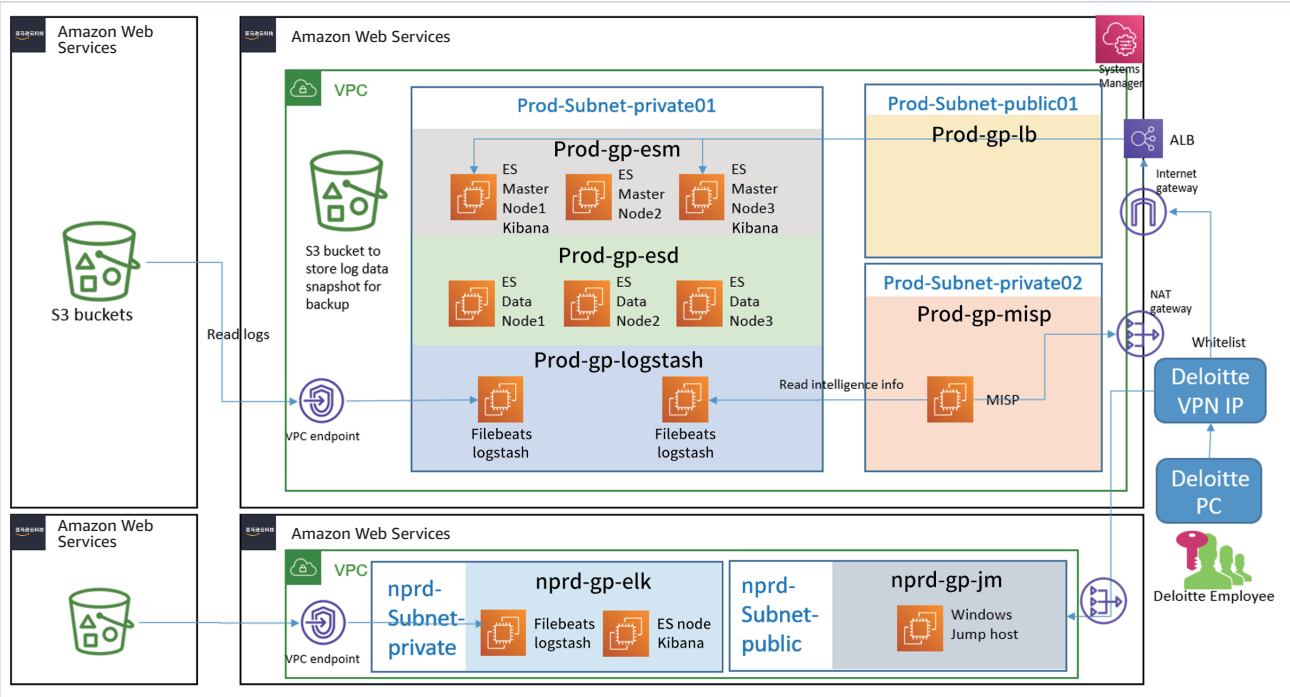
通过安全运营中心，德勤的安全托管服务不但能够快速响应主机、网络、应用及数据等各类安全风险事件，还可以通过实时展示企业安全态势，为企业决策提供支持，实现全栈安全目标，并帮助企业客户满足法律法规的相关要求。

成功案例

德勤为某全球知名的药企客户提供亚马逊云科技云上安全管理服务：

服务内容

- 利用德勤丰富的专业知识、技术和方法，帮助改造和优化组织的 SOC 流程、团队架构和技术平台。
- 帮助客户建设和优化 SOC 平台，包括 SIEM 系统的实施、优化和定制化开发服务。
- 为客户提供一个 SOC 安全团队，快速分析潜在的安全事件，并协助客户采取行动来预防或修复安全事件。
- 提供专门的事件响应和支持服务，满足 SLA。



亚马逊云科技相关服务

和本方案相关的亚马逊云科技主要服务如下：

Deloitte.

德勤Amazon Web Services安全着陆区服务解决方案

应用场景

企业在第一个实际应用上云前，需要有一整套顶层设计和一系列基础框架，以构建一个安全合规的、可以充分信任的、能满足各种业务要求的云环境，为后续的业务上云扫清障碍。业界通常把这些基础框架叫做安全着陆区 (Secure Landing Zone)：

> 企业需要一个合规并符合企业自身安全需求的云基础环境。

> 为用户提供一个安全可信的基础云环境,以进行下一步的系统迁移和应用开发。

> 跨国企业项目需求复杂，待迁移系统复杂。

德勤帮助客户在亚马逊云科技上加速构建安全可信、合规，能够适用于不同部门，灵活可扩展的云上着陆区。

痛点和需求

企业在实际应用上云前，往往需要构建一个安全合规的云上环境，以支持内部不同用户资源的访问控制，成本控制，云上与本地数据中心的安全网络连接，安全审计等安全需求。

企业在云上的合规需求
（LOB / IT）

企业不同部门有各自独立工作环境的需要
（IT / InfoSec）

合适的权限控制并满足追溯和审计要求
（IT / InfoSec）

常见问题和切入点

> 一些相关的典型的客户常见问题如下：

- 云上如何组织账号满足资源管理需求?
- 如何构建云上网络满足安全需求?
- 如何集中管理权限和日志等确保云上安全?

方案价值和客户收益

本方案将德勤在咨询和交付服务等领域的专业咨询能力和最佳实践，同亚马逊云科技云上的先进技术以及第三方安全产品相结合：

基于最佳实践，为用户提供一个安全可配置的企业级云资源环境，满足合规需求。

保证可扩展性，为后续的云迁移和应用开发奠定基础，加速数字化进程。

理解不同行业和地域的安全需求，具有一站式的咨询和交付经验。

方案介绍

德勤结合行业理解和对安全合规实践经验，基于亚马逊云科技最佳实践构造了易于部署的自动化云上着陆区的解决方案，帮助客户快速构建新的合规环境，以支持客户在亚马逊云科技云上运行安全且可扩展的工作负载。

多账号管理

- 基于亚马逊云科技最佳实践的安全、可扩展的多账户亚马逊云科技环境。
- 用于创建多账户环境和构建基线的框架。
- 基于通用安全性的初始多账户结构示例。
- 审核和共享服务要求。
- 支持使用一组安全基线自动部署其他账户。

财务管理

- 管理云平台的合同、优惠、付款关系、账单，以及认证公司在云平台的实体、发票抬头等财务相关的属性。

网络规划

- 规划云上 VPC 的拓扑结构、混合云网络的互联、网络的流量走向、相关的安全措施，以及如何构建高可用和可扩展的网络架构。

身份权限

- 身份权限规划谁能够访问云，并通过单点登录 SSO 和细粒度授权实现人员按需访问。
- 多个账户和定义跨账户角色允许跨所有账户实现职责分离。
- 初始账户安全性和亚马逊云科技配置规则基准。

安全合规

- 安全防护通过在云上构建基础的安全环境，帮助业务系统在云上快速的安全落地。
- 合规审计设计治理的目标和流程，并通过相应的工具来实现对于治理规则的监督。

方案根据在亚马逊云科技在中国区的服务和功能可用性，实现亚马逊云科技网络设计、多账户结构的最佳实践，兼顾考虑了未来服务的通用性。例如，通过 IAM Permissions Boundary 替代 SCP，通过 Cross Account Resource Sharing 来替代 Organization RAM 以及通过 ISV 的产品来帮助搭建 VPN 等。

成功案例

德勤成功地为某制造型企业实施安全着陆区解决方案，通过自动化的方案，为后续的应用在云上的部署和云上的云资源管理和运营等建立基础。

诉求&痛点

由于亚马逊云科技中国区 Control Tower 服务的限制，客户希望在亚马逊云科技中国实施 Landing Zone 搭建多账户架构并建立安全基线和管控以满足服务配置需求的复杂性，并为 SCP 和 AVM 启用替代解决方案。

解决方案

- ❑ 德勤为 Landing Zone 实施提供架构设计和技术实施支持。
- ❑ 依据最佳实践设计多账户组织结构，以实现日志记录和安全监控的集中管理功能。
- ❑ 利用 IaC（Terraform 和 CloudFormation 代码）部署解决方案。
- ❑ 使用 AVM 和 SCP 替代解决方案自动配置新账号安全基线和权限管理。

结果

- ❑ 效率 - 通过利用包含亚马逊云科技最佳实践的自动化且安全的解决方案，缩短了亚马逊云科技入门所需的时间。
- ❑ 敏捷性 - 实现账号级别的控制，并按需为最终用户启动新环境。
- ❑ 集中管理 - 实现核心账号监控所有成员账号活动（包括云消耗）。

亚马逊云科技相关服务

亚马逊云科技的技术架构保证了它可以为客户提供灵活、安全的云计算环境。德勤会根据客户的实际需求灵活配置云上原生服务和第三方安全服务，以满足企业的合规和管控要求。和本方案相关的亚马逊云科技主要服务如下：

- Amazon Security Hub
- Amazon Organizations
- Amazon Control Tower
- Amazon Trusted Advisor
- Amazon Service Catalog
- Amazon Config
- Amazon Well-Architected Tool
- Amazon Systems Manager
- Amazon GuardDuty
- Amazon Macie

德勤隐私合规自评估工具D.PAsS解决方案

首期将上线针对于欧盟《通用数据保护条例》(GDPR)的自评估模块，未来将陆续覆盖其他国家或区域的合规要求。

随着全球化进程加快，越来越多的中资企业选择出海。但海外监管环境复杂多变，中国与海外的监管环境存在一定差异，中资企业在出海过程中将面临各种合规风险挑战。

为帮助出海企业更好地应对此类挑战，德勤基于多年网络安全与合规服务经验打造了隐私合规自评估工具 D.PAsS，帮助您的企业准确识别、持续评估企业在公司管理架构以及产品设计方面的合规情况，提供可采取的优化行动建议。

痛点及需求

出海欧盟过程中，GDPR 多维度的合规要求和其严厉地执法带来了多层次的合规挑战。企业需关注的事项既覆盖在经营过程中面对监管、面对用户所需采取的行动，也包含对于第三方合作伙伴和供应商的管理，以及在经营管理和产品生命周期内的隐私合规行动。

合规面向主体	相关合规要求	常见挑战
监管	• 数据保护官 DPO • 隐私事件处理 • 救济、责任与罚则	• 数据保护官是否已设立并对外公开 • 若发生数据泄漏事件是否可及时上报监管部门 • 是否了解企业内部的风险状况
用户	• 数据主体权利	• 是否有渠道回应数据主体的隐私权利请求 • 删除数据主体的个人数据的方式及场景
管理层	• 数据保护官 DPO • 隐私事件处理 • 跨境数据传输	• DPO 的地位与职责是否可支持其工作开展 • 隐私事件应急处理流程是否完备 • 如何合规地进行数据跨境传输
产品及服务	• 隐私政策 • 默认隐私设计 PbD • 数据安全控制 • 数据保护影响评估 DPIA	• 是否全面、清晰告知数据主体数据处理过程及后果 • 开发产品时如何确定需满足的隐私合规要求 • 目前采取的数据安全措施是否合理 • 数据处理会对数据主体产生什么影响
第三方	• 第三方管理	• 如何约定企业和第三方的责任和义务

产品价值呈现

安全简便的工具部署

- 企业可在亚马逊云科技 Marketplace **一键购买和部署** D.PAsS
- 支持部署企业自身云环境，**无需担心企业业务数据回传**

“化繁为简”的合规自评估工具

- 支持**识别产品/系统与 GDPR 合规要求的差距**
- 通过**点选选项即可**快速获悉企业的隐私合规情况
- 支持接入 Amazon Config* 工具进行**自动识别合规状态**

多维度识别合规差异

- 基于 **GDPR 关注的重点合规场景**，提供 **30 类**隐私合规子类、**100+** 隐私处罚案例，精准识别自身合规差异
- 通过**图形可视化形式**展示各维度自评估结果，提供分析报告

包含合规专家咨询服务

- 产品订阅期间，**可不限次开展自评估并下载分析报告**
- 价格包含**指定人天的专家咨询服务支持**

常见问题和切入点

*该功能需单独购买 Amazon Config 产品。

适用行业广泛

金融	IT	信息通讯	建筑
医疗	安全	教育	广告
电力设备	游戏	电商	物流
工业	旅游	媒体	制造

适用于企业出海各阶段

出海前准备	已出海	退出出海业务

适用场景

出海前准备	已出海	退出出海业务
识别新业务是否受到监管	业务变化时的适用性判断	识别退出后业务是否残余合规风险
识别需构建的合规管理机制	持续跟踪最新处罚案例的重点关注领域	识别退出区域可减少的合规投入
识别新产品需满足的合规要求	产品重大变更后的合规状态自评	分析如何合规地处置业务产生数据

案例

出海业务合规评估

行业

某跨境电商公司

需求

- 产品设计时，提供了欧盟用户访问并下单的功能，是否需满足 GDPR 的要求
- 若需满足，应采取什么行动

持续合规评估

行业

某消费品制造公司

需求

- 期望树立良好品牌形象，持续关注监管热点
- 产品软件版本更新较快，需要持续识别合规性

新技术实践合规评估

行业

某智能制造企业

需求

- 计划撤出欧盟市场，判断是否可以将数据转移到其他区域
- 撤出后数据主体权利响应应满足的要求

应用场景

开展**自评估**：

- 了解业务是否需遵循 GDPR 的要求
- 识别企业需开展的合规提升行动

应用场景

开展**自评估**：

- 识别当前合规状态，了解监管处罚的热点领域

借助**自动化评估辅助功能**：

- 记录资源配置更改以及潜在差异

应用场景

开展**自评估**：

- 识别是否属于监管的跨境数据转移场景
- 识别维护数据仍需满足的合规需求

D.PAsS 页面展示

自评估问卷填写

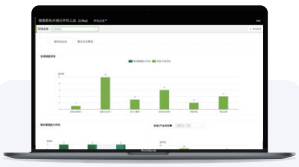
评估问卷为单选点选方式，**降低评估使用门槛**

Amazon Config 检测

嵌入 Amazon Config，**获悉云环境实际状况**

报告导出

多种维度的统计报告供下载，**提供多种场景的汇报支持**



评估总览

汇总至实体层级，**轻松洞悉企业整体合规状况**

提供两种时长套餐

半年套餐

服务时长：6 个月

- 享有 2 人天的远程/上门咨询服务
- 服务期间可无限次使用自评估模块并下载报告

全年套餐

服务时长：12 个月

- 享有 5 人天的远程/上门咨询服务
- 服务期间可无限次使用自评估模块并下载报告

联系我们

联系邮箱：raccp@deloitte.com.cn

NTT MSSP安全托管服务解决方案

应用场景

企业在使用马逊云科技产品开展其业务时，为确保合规和控制自身风险、需要对自身业务系统和相应的亚马逊云科技架构进行有效的安全管理。

客户需要覆盖安全的整个生命周期的托管服务，以帮助企业实现IT安全可视化和可成功执行的安全计划，NTT 根据客户的业务策略制定战略和路线图，量化风险和机会，当面临突发安全事件时，NTT 利用可靠的保障服务来确保安全措施正常运作。

痛点和需求

合规和监管要求远高于自身能力

《中国网络安全法》、《网络安全等级保护条例》、《个人信息保护法（草案）》等等的推出，信息安全快速成为每个企业的必修课

安全事件成本剧增

勒索事件、数据外泄、合规风险等等，使企业面临事件成本，其中包括经济损失、商誉、公信力和市场质疑

常见问题和切入点

- 企业缺乏安全专业人员，难以高效的满足合规要求；
- 安全事件频出，信息安全风险对企业自身业务产生了绝大的隐患。

方案价值和客户收益

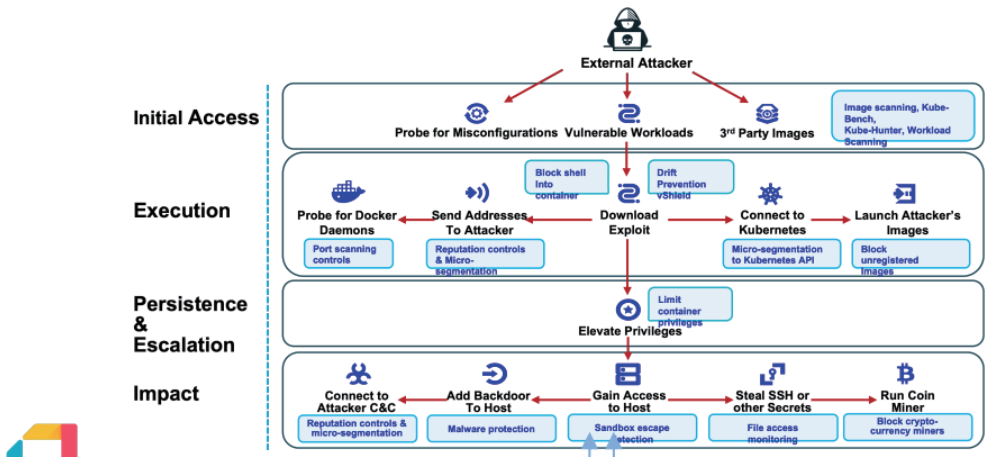
通过 MSSP 方式将安全顾问和专家能力赋予企业，应对合规相关问题，降低整体信息安全风险

信息安全能力的提升也可以有效提升企业对外业务公信力和形象

方案介绍

涵盖托管式安全服务，其独特的设计旨在保护、监控和响应重要亚马逊云科技资源的安全事件，并且作为全天候完全托管式服务交付给客户。有利于监控任何规模亚马逊云科技环境中的安保状况。

统一集中化的 7*24 安全运营中心（SOC）帮助企业监控、分析和响应安全事件；同时安全分析师团队通过对以上 Aqua 安全功能组合的理解和运用，保持管理策略优化和最佳实践。



Protect the Build

漏洞扫描和管理
动态威胁分析
DevSecOps自动化
CI/CD集成

Protect the Infrastructure

合规化管理
Kuberntes集群风险管理
配置审计
混合云和多云架构

Protect the Workload

镜像和运行合规化管理
构建不可变基础设施
流量可视化与微隔离
漏洞影响的控制

管理和实践

Aqua最佳实践管理
Aqua平台持续调优
安全事件及更新管理
CI/CD集成管理

实时监控、分析和响应

日志管理、安全数据存储/数据处理/解析
安全可视化/7x24 实时监控
漏洞分析和评估
威胁分析/关联分析/深度分析

周期性报告

安全事件调查报告
漏洞分析和评估报告
月度安全洞察报告
周期性安全简报

成功案例

某国际零售行业公司，亚马逊云科技使用 500 台以上 EC2 主机和相关基于亚马逊云科技网络层应用。

我们 MSSP 托管服务，帮助用户进行基础设施漏洞扫描和管理，凭借托管式端点检测和响应和托管式的 WAF 帮助用户有效控制攻击面，监控潜在威胁和分析安全事件。

亚马逊云科技相关服务

主要涉及的亚马逊云科技服务：

Amazon CloudTrail

Amazon GuardDuty

Amazon Identity & Access Management (IAM)

Amazon WAF

NTT SIEM安全信息和事件管理解决方案

应用场景

NTT 安全运营平台的日志监控服务可以及时准确地识别与安全相关的事件，以确保您对有效威胁做出响应，确保您正在应用正确的响应，并确保您的关键资产始终得到适当的保护。

借助网络防火墙，入侵检测和防御系统（IDS/IPS），VPN，路由器和交换机，关键业务系统，非关键服务器以及组织中过多的端点生成大量日志等设备和技术，几乎不可能识别与安全相关的事件与不安全的事件之间的区别。

痛点和需求

安全事件量日益增大

多种多样的安全和系统产生大量的告警、日志和事件，需要专业系统对安全事件和信息进行统一管理

安全事件缺乏人员进行监控、分析和跟进

通常需要 7x24 全天候关注和分析，并及时和客户沟通进行响应

常见问题和切入点

- 合规驱动，安全日志保存市场要求
- 事件量过大，没有专业系统和人员进行处理

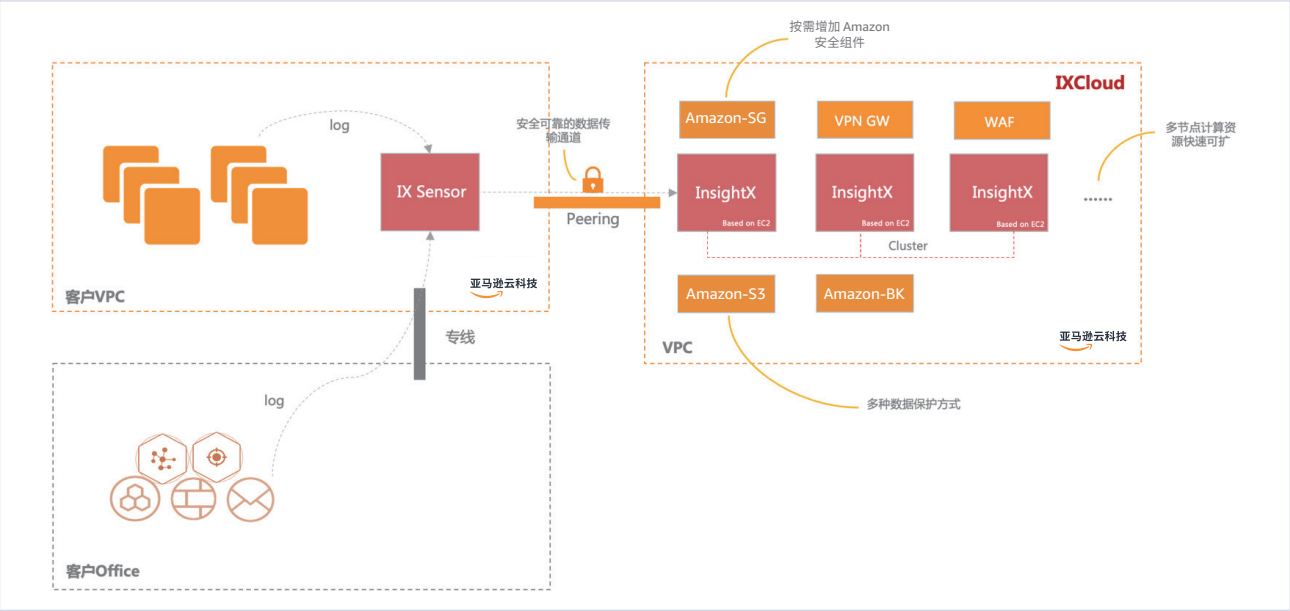
方案价值和客户收益

通过基于亚马逊云科技的云原生 SIEM 平台，并通过托管式的 SOC 服务帮助用户高效快速进行安全事件的收集、监控和分析

方案介绍

通过基于亚马逊云科技的云端 SIEM 平台对用户的 IT 环境进行安全事件和信息管理

通过统一集中化的 SOC 中心帮助企业监控、分析和响应安全事件和问题。这个其中结合了人员、流程、技术和数据，帮助客户实现全面的安全性。同时，无论是企业内部还是公有云 VPC，IX 按需部署或者 IXCloud 方式，均可灵活实现安全运营需求。



成功案例

帮助某能源企业所有亚马逊云科技相关安全组件和系统、包括 Amazon ECS 相关系统安全数据、均通过我们 SIEM 安全分析平台进行统一收集、处理、监控、分析。

同时安全分析专家团队 7x24 全天候进行值守和威胁分析、帮助用户在大量的安全告警中关注真正威胁事件、并通过事件报告和周期性报告提升安全管理效率和能力。

亚马逊云科技相关服务

主要涉及的亚马逊云科技服务：

Amazon EC2　Amazon S3　Amazon Load Balancing　Amazon CloudTrail　Amazon GuardDuty　Amazon WAF

NRI基于亚马逊云科技的安全准则制定咨询服务解决方案

应用场景

随着网络安全法和个人信息保护法的生效，在中国大陆部署的 IT 系统，安全方面的重要性也与日俱增。利用亚马逊云科技服务，考虑安全性时，除了传统的措施（以防火墙和 WAF 为代表的网络边界保护、防病毒或其他终端节点安全），作为基础的云服务层的安全也是非常重要的。

亚马逊云科技提供了许多优质的安全服务。

痛点和需求

'咦，存储在 S3 中的市场数据不是可以从互联网上参考吗?'
'亚马逊云科技资源使用费用异常的高??高性能的实例长时间在运行。咦，虚拟货币的挖矿程序正在运行.....'

正是为了防止此种类型的事故发生，亚马逊云科技提供了很多优质的安全服务。
然而，通过在企业内使用这些服务，从而建立一个安全的云环境有许多的课题。

> 如何将企业内的统一管理规范及安全策略实际安装到亚马逊云科技服务中。

> 如何将专家的见解及云上的最佳实践落地。

北京 NRI 提供这些问题的解决服务，以及为了安全的使用亚马逊云科技服务，应如何制定安全准则的咨询服务。服务对象包括从企业内部负责 IT 系统统一管理的信息部门，到利用亚马逊云科技独自展开业务的事业部门。

方案介绍

通过参照行业标准的最佳实践基准，并且纳入 NRI 集团（全球）积累的经验，对安全准则的制定提供支援服务。基于 NRI 标准准则和各个企业的安全准则，也可以提供个性化的定制服务。

此外，为了不让安全准则变成“画饼”，对实施的环境进行评估及改善，建立流程管理是非常重要的。因此，NRI 北京不仅制定安全准则，还提供对设定项目的自动化检查以及实施环境是否遵守了安全准则的监控服务。如果有违反安全准则的情况存在，将会立即被检测到并且会立即报警，是比亚马逊云科技的安全服务更高出一层的服务。

对行业标准的见解·加之亚马逊云科技最佳实践以及 NRI 积累的经验的利用。

可以根据客户的安全政策和战略进行个性化定制。

在 DevSecOps 环境下，能够实现对安全准则遵守情况的自动监视。

指导方针的构成要素	记载内容	记载分类
云利用方针	从安全策略导出的云利用方针	各公司方针
假想的威胁	从现实世界中观测到的网络攻击的信息。 (来源：美国MITRE ATT&CK知识库)	最佳实践
基线对策	组织应采取的 “最低” 程度的基线措施。 (来源：美国CIS Controls)。	
事实标准对策	为了安全的建立和维持信息系统的行业标准对策。 (来源：美国CIS Benchmarks)。	
亚马逊云科技推荐对策	在安全、隐私和合规方面的安全原则及管理的最佳实践 (来源:Amazon Well-Architected Framework)	
应实施的具体对策	要执行的亚马逊云科技及其配置项目。	NRI经验 +各公司对策
对策的优先顺序	根据信息的敏感性来确定对策的优先次序。 SHALL/MUST/SHOULD/BETTER	

亚马逊云科技相关服务

和本方案相关的亚马逊云科技主要服务如下：

被监控资源和安全服务

HITACHI
Inspire the Next

日立解决方案（中国）有限公司
IT资产管理解决方案

应用场景

当初作为公司经营资产而购买的 PC、服务器、软件等都用的公司经费。如果连这些资产的“什么时候，由谁，花多少钱买的，买给谁用”都不明确的话，就很有可能在会计审查与内部管理上发现问题。

使用未经授权的软件或不法复制行为是违反法律法规的。在许多软件厂商的产品使用上，还将牵涉到该厂商的许可证审查等条件。可以说几乎所有使用软件的公司都会受到相关的许可证审查要求。每天为了应付意料不到的审查要求本身风险就很大，如果一旦被查到不法使用，将会蒙受莫大的损失。

对于许多企业而言，机密信息一旦泄露了便会直接丧失公司的社会信用。特别是对于个人信息的处理，如何避免个人信息泄露早已成为一个重大课题。必须通过 PC 操作实施获取调取的操作监控以及采取各种使用权限等对策。

痛点和需求

随着商务经营环境的多样化与复杂化，对于 IT 资产的管理(掌控)越来越重要。

- IT 资产管理的不彻底
- 侵权或违规
- 安全事故
- 病毒感染

常见问题和切入点

一些相关的典型的客户常见问题如下：

- 需要完善资产管理
- 需要完善软件许可证管理
- 需要完善信息防漏措施

方案价值和客户收益

- 自动收集最新的资产信息；
- 一旦发生情况变化后便可一目了然实时掌控；
- 对于不经常连接网络的笔记本电脑及智能设备产品也可实施管理；
- 管理许可证使用情况(许可设备、许可证均可实现统一匹配) 另外，可自动提前通知接近使用期限的情况。

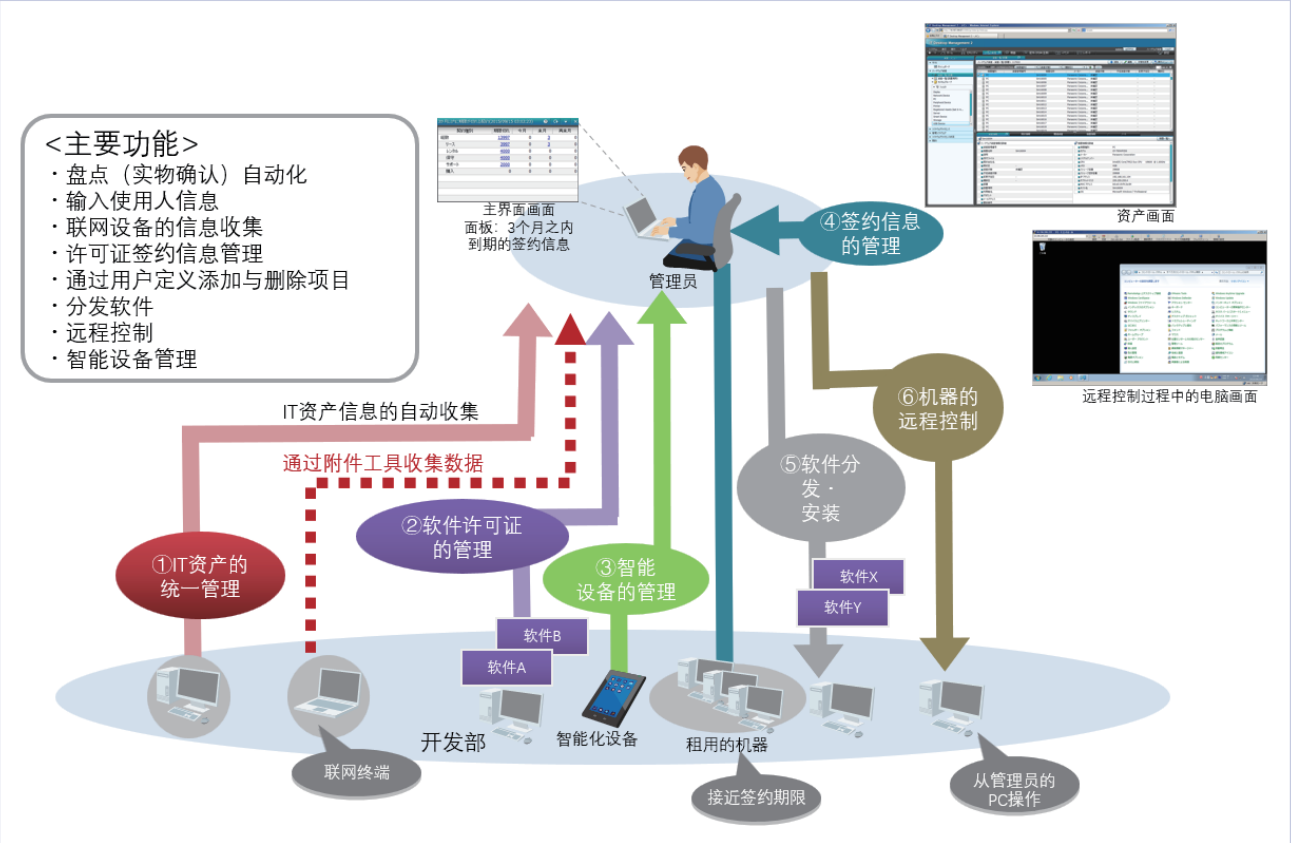
- 当发现擅自安装软件时，自动发出通知；
- 与现有的许可证数量对比，确认匹配数量。

- 监控电子文件的带出操作；
- 控制电子文件的取用；
- 确认病毒防控产品的状态及定义文件是否已更新；
- 确认 Windows 更新程序(补丁)是否已更新；另外，可确认 OS 设定中有无问题；
- 可屏蔽未经批准的机器连接网络；
- 当发现新软件后，可立即在主界面画面上显示。

方案介绍

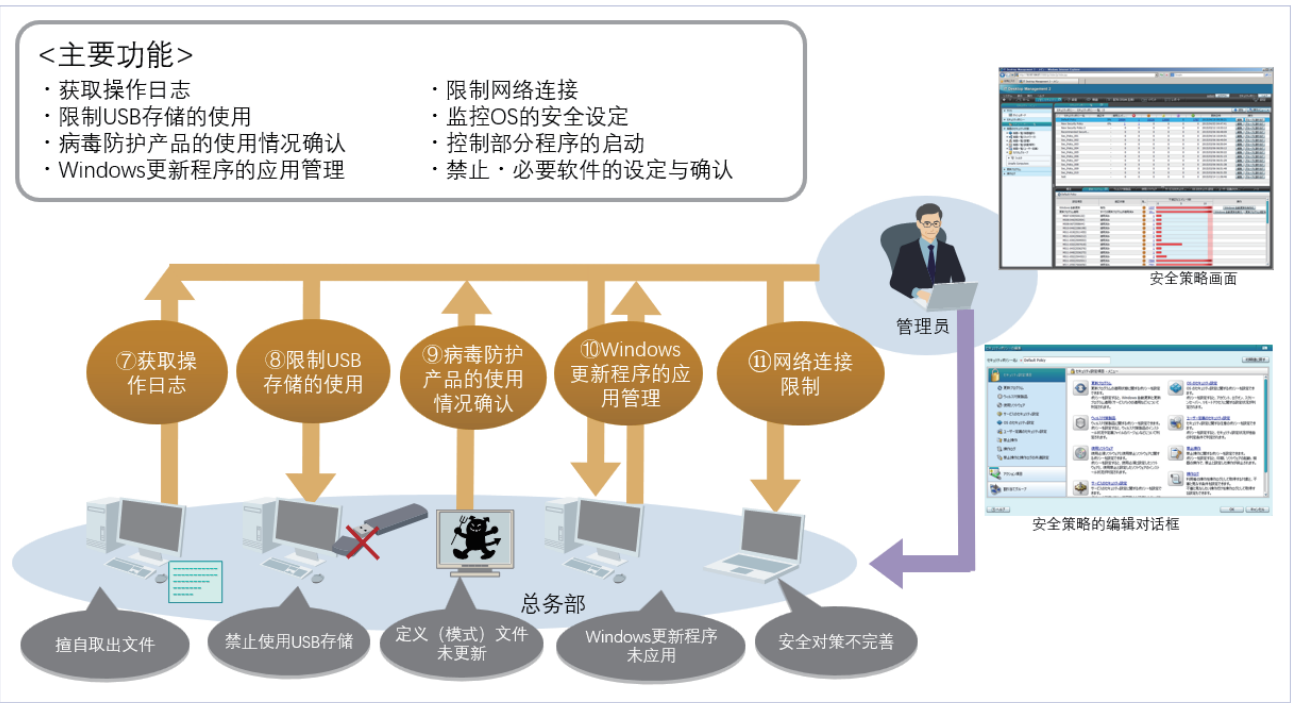
IT 资产管理的应用场景

统一收集公司内部的 IT 资产信息并实施管理。有助于提高管理效率并确保准确的 IT 资产管理。



安全管理的应用场景

可高效确认统一整合后的 IT 资产信息与安全策略。并且，随时确认各个 PC 与 PC 服务器的安全对策信息，并依此采取相应措施。



成功案例

行业	规模	要件	顾客的课题	导入的好处
金融业	18 据点	设备管理	由于通过 Excel 表手工管理台式 PC 及笔记本 PC 的 IT 资产，当发生采购或报废，IT 资产信息变更的时候，经常发生信息遗漏的情况。	由于管理所需的信息都是自动收集，因此还没有进行登记的新设备的发现，以及经过一段时间不知道是否还存在的设备信息的掌握就变得很简单。
			由于 PC 等 IT 资产分布在分散的各个据点，各据点的 IT 资产信息的收集依赖于各据点担当人员的自我汇报，很难做到信息收集的准确性。	IT 资产的盘点信息从各个据点自动收集上来，实现了不依赖于担当者汇报的信息的准确性。
		安全管理（USB 控制）	随着 USB 设备使用频率的增加，终端用户在 PC 上使用个人 USB 设备感染病毒的风险也随之增高。	通过禁止管理对象外的 USB 设备的使用，大大减少了感染病毒的风险。
		网络访问控制	因为有客户的重要信息，非常担心公司内由于非法访问造成的信息泄露。	通过对网络访问的控制，从公司外带来的 PC 在没有许可的情况下，不能访问公司的内部网络。从而大大降低了信息泄露的风险。
制造业	约 10,000 台	设备管理	虽然日本国内据点做到了 PC 的管理，但是在海外据点，因为没有导入管理工具，没有实现 PC 的管理。	国内据点和海外据点实现了 PC 的统一管理。
		使用者信息的收集	因为不能掌握 PC 使用者的信息，盘点作业的效率很差。由于部门变更等原因，PC 的使用者信息就会改变，掌握最新的信息变得很困难。	PC 和使用者的关联信息由使用者本人进行维护，信息的管理变得简单，盘点作业的效率也大大提高了。
		HelpDesk（远程操作）	海外据点的 PC 出现问题的时候，HelpDesk 只能进行电话对应，从状况的掌握到问题的解决要花很长时间。	通过远程操作，可以看到并操作出现问题的 PC 的画面，解决问题的效率大大提高了。
制造业	约 50,00 台	分发	业务软件在每次导入或更新的时候，都要通过手工分发，非常麻烦。不同使用者的业务软件的版本不一样，PC 出问题的时候，就需要耗费 HelpDesk 很长的时间进行对应。	由于 JP1 有软件分发的功能，就可以使公司内所有必须安装的软件的导入和版本保持一致，大大减少了故障发生的频率。
		License 管理	由于不能正确掌握已安装的软件数量，使用状况的调查要花费很多时间。无法快速响应软件厂商的 License 对应。	对已安装软件的信息可以进行自动的收集和统计，License 使用状况的调查结果报告很容易就可以做成了。
		操作日志的获取	为了防止信息泄露，希望能对 PC 使用者对文件的操作进行记录，但是过去没有办法。	通过对 PC 使用者对文件进行操作的日志记录，就可以掌握类似把文件拷贝到外部介质等信息泄露的操作。

亚马逊云科技相关服务

JP1 系统支持多种模式部署。部署时可以结合亚马逊云科技系统，利用其弹性伸缩服务，不仅可以降低运维成本，还因为其优秀的扩展能力，可以进一步根据业务需求，动态调整应用程序的容量，提高了系统的灵活性和扩展性。其次在亚马逊云科技的高可用性及容错性服务的加持之下，进一步提高了 JP1 系统的高可用性和可靠性，保障了业务系统的连续性和稳定性。

HITACHI
Inspire the Next

日立解决方案（中国）有限公司
SOC（安全运营中心）解决方案

应用场景

在不可逆的数字化浪潮中，传统的网络边界持续瓦解，更需要我们建设融合覆盖数据安全、云安全等的安全能力，为企业的长足发展保驾护航。

SOC（安全运营中心）基于基础安全架构，结合威胁情报、态势感知等新技术实现安全协同、风险预警、管理闭环的安全能力，进一步健全网络安全综合防御体系。近年来被广泛应用于以下场景：

> 针对企业的网络攻击不断趋于复杂化，带来的损害也呈指数级增长。这类攻击的主要目的是盗取企业的高价值信息资产，危害巨大。SOC 可以为企业构筑安全防线，抵御复杂的网络攻击。

> 《网络安全法》、《数据安全法》、《个人信息保护法》等法律的出台和监管措施的强化，使得网络安全建设的导向已从传统的被动防御转变为主动防御体系。SOC 帮助企业紧随政策及时调整安全建设的思路。

> 随着企业安全业务的发展，越来越多的安全工具、安全对策不断堆叠，难以充分发挥最大效力。SOC 的构建帮助企业有效整合安全工具。

痛点和需求

针对企业的网络攻击（如目标攻击等）不断趋于复杂化，带来的损害也呈指数级增长。这类攻击往往使用未知的恶意软件，所以难以仅通过传统的网络安全预防措施来应对。这就需要构建新的机制来快速检测和响应攻击。

- 网络攻击趋于复杂化，安全事件层出不穷，传统的安全应对方案逐渐力不从心
- 随着云计算、大数据等新技术的兴起，数字资产数量增多，变动加剧，面临更加复杂的攻击面
- 越来越多的安全工具、安全对策不断堆叠，难以实现有效管理
- 随着《网络安全法》等各项法律政策的出台，需要应对更加严格的合规管理

常见问题和切入点

- 如何建立起一套企业自己的主动安全防御体系，实现 7*24 的监控，可以高效应对各类安全事件，避免攻击带来的损失？
- 如何有效纳管企业的安全工具和各种安全策略，实现有序高效的安全防御？
- 如何紧随国家政策的引导和转变，实现安全策略的调整，从容应对合规义务？

方案价值和客户收益

SOC 将安全技术、流程和管理人进行有机结合。基于基础安全架构，结合威胁情报、态势感知等新技术实现安全协同、风险预警、管理闭环的安全能力，进一步健全网络安全综合防御体系，保障关键信息基础设施、重要网路和数据的安全。

以远程或者本地部署的方式为客户提供持续化的资产监控、提供全面的漏洞监测、事件监测、敏感信息监测等服务。也可根据客户需求辅助客户进行自建 SOC。

日立解决方案（中国）有限公司（以下简称：HSCN）SOC 平台支持多云架构，针对企业云安全提供多种拓展性服务。基于亚马逊云科技（Amazon Web Services）搭建的 SOC 平台，可充分利用亚马逊云科技安全且可自由拓展的服务，利用亚马逊云科技可扩展存储，存储来自用户系统的大量日志，从而强化 SOC 平台的可扩展性，数据可用性等性能，优化用户体验。

安全运营最终能够清晰的了解企业自身安全情况、发现安全威胁、规范安全事件处置情况，提升安全团队整体能力，逐步形成适合企业自身的安全运营体系，并通过成熟的运营体系驱动安全管理工作质量、效率的提高。

方案介绍

SOC（安全运营中心）结合了安全技术、流程和人，基于基础安全架构，结合威胁情报、态势感知等新技术实现安全协同、风险预警、管理闭环的安全能力，进一步健全网络安全综合防御体系，保障关键信息基础设施、重要网路和数据的安全。

基于 SOC 服务流程，我们提供从 SOC 构建的咨询、设计和定义，到运营维护的一系列服务。并且可以根据客户实际的业务需求，针对流程中的特定环节实施服务。

成功案例

项目背景：

- 金融行业的保险公司，对网络及信息安全风险防御能力有较高要求
- 现阶段一部分安全工具有独立部署，但日志的全面收集和分析功能尚未实现

客户需求：

- 需要加强迅速发现安全威胁、快速识别安全事件和分析调查的能力
- 需要伴随安全风险及时调整防御策略，进一步提升风险预测能力

解决方案：

- 构建 SOC 安全日志分析平台，通过安全日志的收集和关联化分析，实现安全防御系统的优化

项目实施流程：

阶段一	阶段二	阶段三	阶段四
平台系统的构建	**安全日志的收集**	**数据源扩展**	**画面表示**
部署通用中继器 采用分层逻辑体系结构，分散放置每个功能模块	Syslog-ng、API 等安全日志的收集 业务监控、分析、展示	安全资产信息，安全信息的拓展 安全场景的设计和关联	安全监控画面 日志检索画面

项目成果：

- 通过安全监控画面实现了对于安全状态的可视化，实现了对于日志的收集和关联化分析功能

亚马逊云科技相关服务

普华永道漏洞扫描解决方案

应用场景

随着云计算技术的快速发展，越来越多的企业选择将 IT 系统迁移到亚马逊云科技等云上。亚马逊云科技(Amazon Web Services)已成为各类企业 IT 基础设施的重要组成部分。如何实现漏洞管理在亚马逊云科技的闭环管理，持续保障云环境的安全稳定，已成为企业安全管理的突出课题。

> 企业需要了解自身的信息安全水平，并缓减和修复安全风险。

> 客户需要对现有的系统实现漏洞闭环管理。

普华永道专家团队作为企业安全能力的“外脑”，充分借鉴行业最佳实践的宝贵经验，诊断当前云资源的安全能力短板，并通过切实的整改方案，弥补技术差距，提升 IT 防御能力，有效抵御纷繁复杂的互联网攻击，持续保障云环境的安全稳定。

痛点和需求

安全性和合规性是亚马逊云科技和客户的共同责任。在责任共担模式中，亚马逊云科技负责“云本身的安全”， 客户负责“云内部的安全”。针对亚马逊云科技基础设施的漏洞管理，客户将面临如下几个突出问题：

- 如何及时准确地识别云上资产的漏洞（InfoSec / IT）
- 如何根据自身的业务特点为漏洞排定修复优先级（IT / InfoSec）
- 补定安装后如何验证漏洞修复有效性（IT / InfoSec）

常见问题和切入点

普华永道基础设施漏洞扫描解决方案在各个行业广泛适用并帮助企业实现降本增效、敏捷创新、安全合规、推动业务。

- 提升防御能力，有效抵御纷繁复杂的互联网攻击
- 实现闭环管理，依靠回归测试检查实现正向 PDCA 循环
- 优化资源配置，帮助客户集中资源解决最紧迫安全问题
- 满足合规要求，定期执行漏洞扫描，降低合规风险

常用的用例

快速发现漏洞

自动发现漏洞并近乎实时地快速将其发送给适当的团队，以便他们立即采取行动。

修复补丁的优先级

使用最新的常见漏洞和暴露 (CVE) 信息结合网络可访问性等因素来创建基于上下文的风险评分，帮助您优先考虑和解决易受攻击的资源。

满足合规性要求

通过扫描支持 NIST CSF、PCI DSS 和其他法规的合规性要求和最佳实践。

更快地识别零日漏洞

通过使用 50 多个漏洞情报源来帮助快速识别零日漏洞，从而加快 MTTR。

方案实现方式

普华永道作为专业的信息安全咨询公司，曾为金融业、互联网业、制造业、医疗及制药业等多家跨国集团提供漏洞评估、渗透测试等信息安全技术评估服务，已沉淀了成熟而完整的漏洞评估方法论。

方案制定	执行扫描	手工验证	汇总报告	回归测试
方案制定 正式启动前充分沟通扫描方案，包括：扫描范围、时间窗口、扫描目标的主机类型、操作系统版本、扫描策略等。	执行扫描 根据沟通确定的扫描方案，顾问团队将使用行业标准扫描器完成漏洞扫描。	手工验证 扫描器完成自动化扫描后，顾问团队将对结果进行手工复核。排除干扰信息，确认漏洞真实性和漏洞潜在风险影响。	汇总报告 参考行业最佳实践，结合客户具体业务特点，整理并交付完整的评估报告，帮助客户理解当前漏洞水平并修复漏洞。	回归测试 在客户完成补丁安装与漏洞修复后，顾问团队将对修复结果进行验证，确认修复措施的有效性

提供完整而科学的漏洞管理，基于网络杀伤链（Cyber Kill Chain）模型，使用自动化工具和手工识别的方法，寻找目标系统中存在的各类漏洞并加以利用，尝试获得初始访问权限或提升已有权限。

普华永道的专业顾问团队是一个由云计算、安全攻防及 IT 运维专家构成的综合团队：

云计算团队

由精通亚马逊云科技的技术专家组成，熟悉亚马逊云科技云架构及云上设备管理，能够针对客户的亚马逊云科技环境量身打造评估方案。

安全攻防团队

由顶级白帽安全专家组成，精通网络攻击与防御技术，熟悉最新漏洞利用与评估技术，熟悉常见漏洞缓解与修复方法。到生产线工位。

IT 运维专家团队

由精通 IT 运维技术专家组成，成员均有多年 IT 运维与架构设计经验，熟悉各行业 IT 特点，帮助团队设计可落地的修复与加固方案。

扫描工具介绍

普华永道将采用行业标准的漏洞扫描器执行前述扫描工作，漏洞扫描器将根据客户实际情况与需求灵活选择商业产品或亚马逊云科技的原生扫描器软件，例如 Amazon Inspector。

亚马逊云科技相关服务

和本方案相关的亚马逊云科技主要服务如下：

Amazon Inspector　Amazon Systems Manager　Amazon CloudWatch　Amazon Security Hub　Amazon EventBridge

刘峰　普华永道网络安全与隐私保护服务资深经理

feng.fa.liu@cn.pwc.com

普华永道隐私保护合规解决方案

中国互联网的发展已经来到了一个新阶段，2022 年 2 月 25 日，中国互联网络信息中心（CNNIC）在京发布第 49 次《中国互联网络发展状况统计报告》（以下简称：《报告》）。《报告》显示，截至 2021 年 12 月，我国网民规模达 10.32 亿，较 2020 年 12 月增长 4296 万，互联网普及率达 73.0%，其中手机网民规模达 10.29 亿，网民使用手机上网的比例高达 99.7%。高活跃的用户群体推动互联网和应用程序使用量创历史新高，截至 2022 年 3 月末，第三方应用商店在架应用分发总量达到 20696 亿次。以海量个人信息为支撑的新业态新模式不断涌现，企业大量收集消费者个人信息用于业务增长。然而，个人信息泄露、违法使用个人信息等问题十分突出，个人信息保护工作刻不容缓。2021 年 11 月 1 日，《个人信息保护法》的出台完善了国内个人信息保护的法治顶层设计，亦强化了个人信息安全的监管环境。仅在 2021 年的 APP 违法违规收集使用个人信息专项治理中，工信部累计开展了 12 批次技术抽检，对 208 万款 APP 进行技术检测，通报了 1549 款违规 APP，下架了 514 款拒不整改的 APP，且多次召集互联网企业召开 APP 个人信息保护监管会，敲响了隐私合规必要性的警钟。2022 年 7 月 7 日，国家互联网信息办公室发布了《数据出境安全评估办法》，并规定该评估办法自 2022 年 9 月 1 日起施行，完善了我国个人信息保护的监管版图，隐私保护与数据安全开始成为备受业界关切的话题，相关议题也成为了各企业合规工作的重中之重。作为专业服务机构，普华永道为企业客户提供全方位的隐私保护合规解决方案，结合亚马逊云科技的先进技术沉淀与普华永道的丰富行业经验，从合规咨询到技术落地，全方位帮助客户识别隐私保护风险，应对隐私合规挑战。

隐私保护合规难点

基于亚马逊云科技服务的普华永道隐私保护合规解决方案致力于帮助客户解决以下合规难点：

法规标准碎片化

各国对于个人信息保护与数据安全的立法并非一蹴即至，而是随着经济技术的发展处于动态更新的状态。法律立法后，相关配套的标准、规范也将不断出台，如《个人信息保护法》中，针对合规审计提出了法律要求，但具体的实施标准却缺乏明确的定义。这样的法律留白需待相关标准、规范文件来完成进一步补充。因此，法律本身与相关配套标准、规范的结合，才构成一整套完整的合规框架。而要理解并落实这样“碎片化”的法律与标准规范，更进一步提升了企业在隐私合规道路上的成本。

隐私合规人才稀缺

虽然近年来方兴未艾的隐私保护立法催生出大量的合规需求，但企业内部往往缺少具备充分经验的合规人才来执行隐私合规管理工作。隐私合规绝不仅仅是对相关法条的生硬解读，而是要在理解业务逻辑、合规要求、技术标准等多方面复合知识的基础之上，精准把控合规风险，正确做出合规判断。因此，合规人才不仅需要复合全面的知识背景，也需要大量行业经验作为支撑。而缺少经验沉淀的企业，很难培养或在短时间内找到合适的隐私合规全职人员开展相关工作。

合规流程繁琐

隐私合规工作的落实绝不仅依赖于合规部门，而是要在合规部门的主导下，协调各业务部门共同协作。在此过程中，各利益相关方的广泛参与无形中增加了合规工作的复杂性。在对内进行充分项目管理的同时，也需要保持与监管部门的有效沟通，并对隐私合规工作的结果进行及时上报。如果无法很好管理隐私合规流程，不仅会干扰到企业业务的正常运作，还可能招致监管处罚。

缺少专业工具

当下企业的隐私合规工作大多依赖于线下人工操作，对于合规问题的判断缺少系统化工具的辅助支持，进而影响隐私合规管理的效率与质量。此外，企业内部各部门之间缺少统一的隐私合规管理线上协作入口，导致隐私评估工作流分散，以及评估记录的碎片化，难以形成有效的监管应对。

方案实现

针对以上合规难点，普华永道从合规咨询与技术落地两方面出发，提出全方位的企业隐私保护合规解决方案。

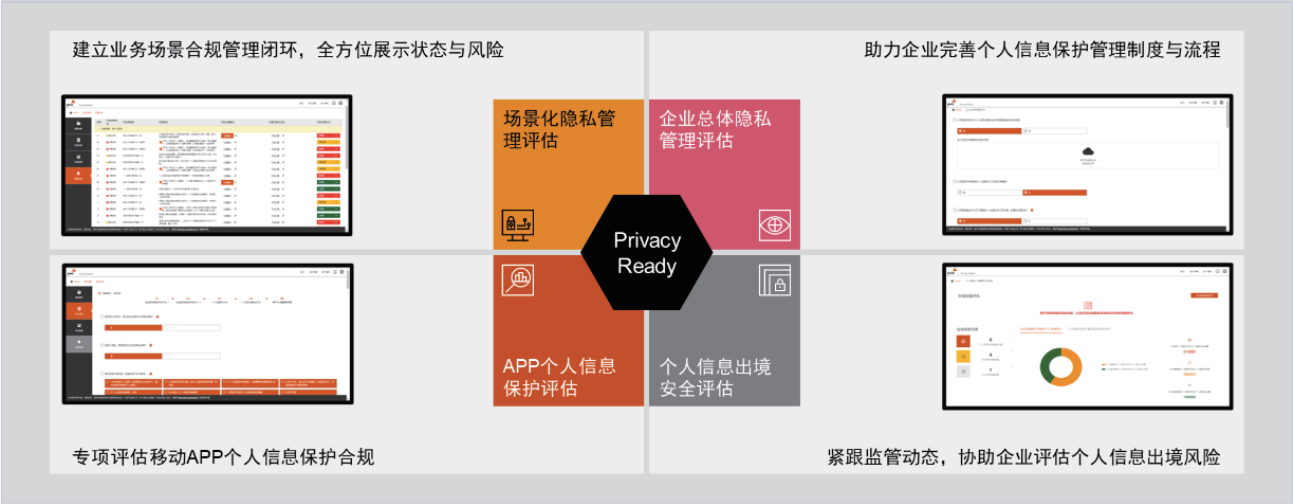
➤ 隐私合规咨询服务

在隐私合规咨询服务中，普华永道将帮助企业识别现有的个人信息处理活动及涉及的相关系统，清楚了解个人信息收集、存储、使用、销毁、共享、跨境传输等处理场景，梳理个人信息全生命周期中的风险情况。在此基础之上，普华永道将对标适用的法规与标准、指南，开展差距评估，明确合规差距。对识别出的差距进行评估，针对性地提出改进建议，如修订隐私政策、加强访问控制、对个人信息进行去标识化处理、建立数据资产清单等。最终，在公司治理层面，建立个人信息合规管理的长效机制，通过协助确立个人信息保护岗位职责并落实个人信息管理体系（Personal Information Management System, PIMS）等方式，强化公司隐私设计（Privacy by Design, PbD）能力，让隐私保护与公司日常运营的全阶段相结合，积极主动地构建端到端的隐私安全生命周期保护机制，满足法律法规与企业的隐私合规要求。

➤ 合规评估专业工具

普华永道致力于将数字化工具应用于项目实践，以实现更有效率的隐私合规改进。针对企业的隐私合规痛点与监管趋势，普华永道自主研发并推出一款数字化中国个人信息保护合规管理平台——Privacy Ready，帮助企业梳理个人信息处理活动，及时识别业务合规问题，持续监控风险处置进程，赋能企业个人信息合规管理。

Privacy Ready 兼具企业总体隐私管理和具体业务场景隐私合规评估能力，并重点突出数据跨境传输合规评估、移动 App 个人信息保护评估等监管重点，能够全方位展示风险态势，并持续追踪整改状态。



图片来源: 普华永道 Privacy Ready 截图

Privacy Ready 六大核心功能包括

- **自动化评估流程：**

  基于个人信息保护法要求，设计直观易懂的自查问卷，快速排查具体业务场景的个人信息保护合规风险。

- **自动生成风险看板：**

  内置风险因子和规则引擎，一键自动生成合规问题与风险矩阵，简洁易懂的风险看板助力企业管理合规风险。

- **可视化追踪风险处置：**

  可视化追踪风险处置进度及持续改进计划，构建发现、评估、整改、优化的管理闭环。

- **全方位展示数据资产：**

  自动根据评估场景生成资产清单，提供响应监管要求的个人信息收集清单、系统清单、与第三方共享个人信息清单。

- **一键生成评估报告：**

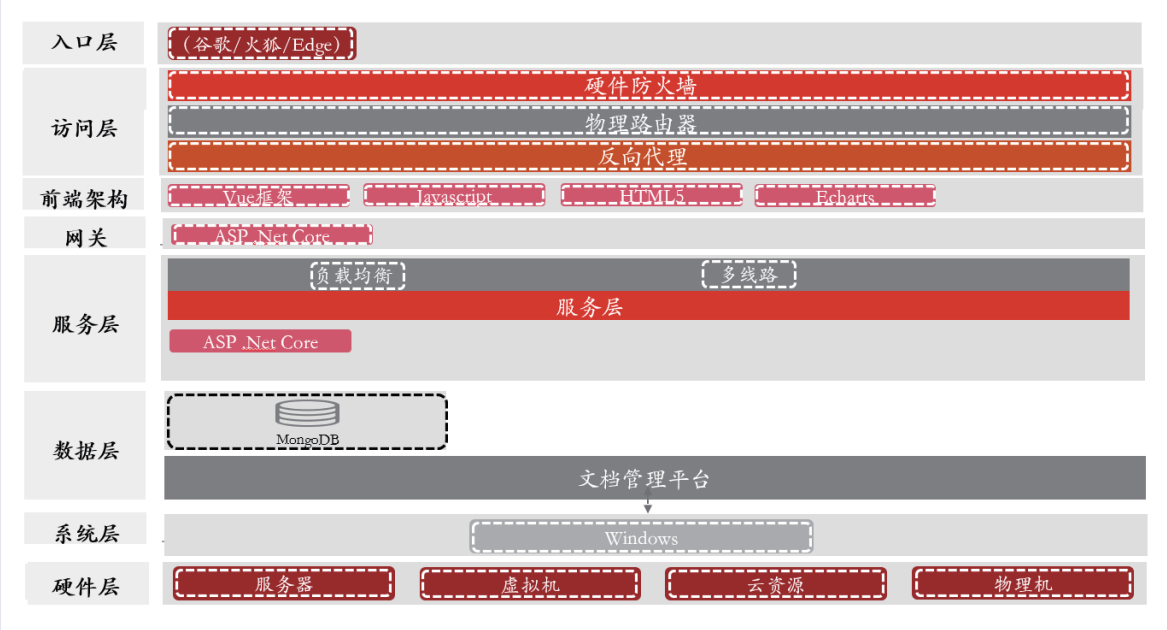
  一键生成个人信息安全影响评估报告，完整记录评估流程和结果。

- **个人信息出境管理：**

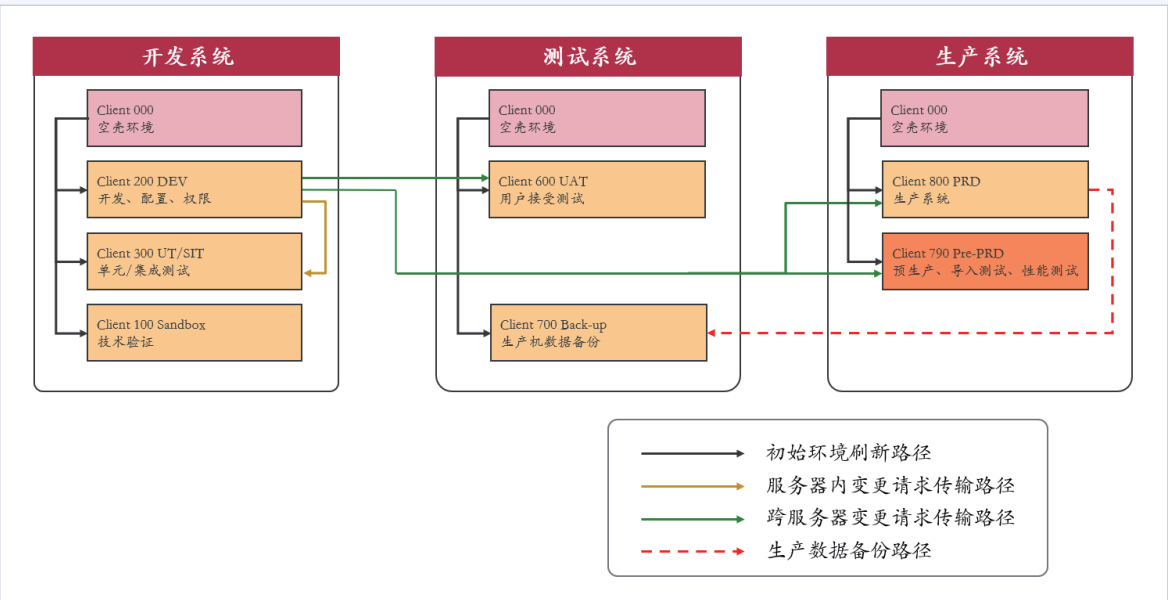
  自动统计企业个人信息出境的场景、出境个人信息数量与出境目的地，协助企业管理数据出境风险。

方案架构

PwC Privacy Ready 系统架构图

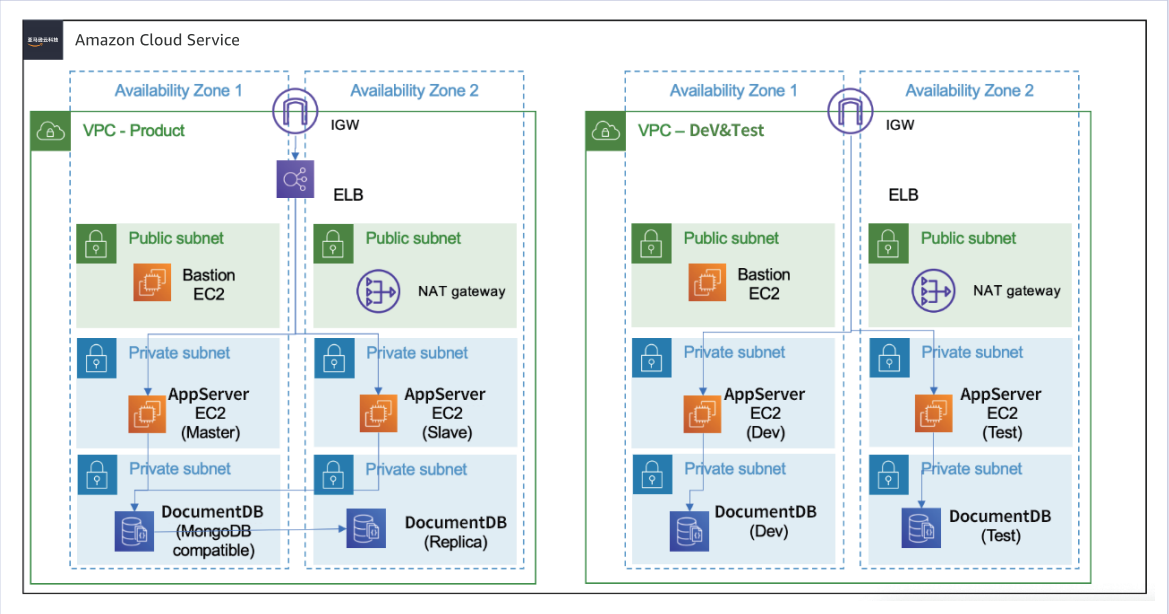


PwC Privacy Ready 的系统环境分布和传输策略



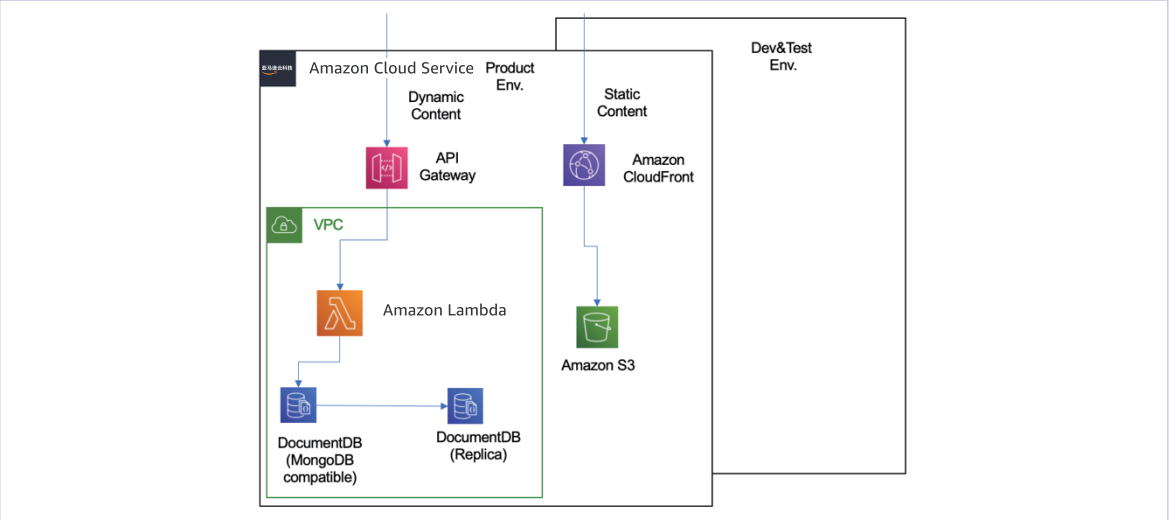
Privacy Ready on 亚马逊云科技快速部署架构

Privacy Ready on 亚马逊云科技快速部署模式，将 Privacy Ready 系统部署到云上主机环境，在云上提供生产环境和开发测试环境这两个环境。生产环境中，两台 EC2 云主机达成高可用，且通过部署一个主 DocumentDB 和一个副本进行热备份。



Privacy Ready on 亚马逊云科技无服务器技术部署架构（中长期规划）

为了更好地利用亚马逊云科技云的技术优势和新型的服务与架构，在 Privacy Ready 的中长期规划中，考虑使用无服务器技术的部署架构。客户访问的静态页面可以通过 S3 的静态页面的功能实现，动态的内容使用 API Gateway加上 Lambda 再加上 DocumentDB 的架构，来取代原先的 EC2 上部署应用服务器的架构。架构图如下图所示。



方案优势

行业经验沉淀

普华永道网络安全与隐私保护团队与亚马逊云科技在合规实践方面有深厚的合作经验，凭借多年的积累，已建立起了针对世界各国主要隐私法律的合规实践方法论，涵盖范围包括了 GDPR, PIPL 及相关标准、规范，满足不同客户的隐私合规需求。此外，普华永道也与行业专家及学者保持积极交流，能够为客户带来隐私合规的深入解读与前沿视角。

专业人员团队

普华永道网络安全与隐私保护团队在全球有超过 4,500 名专业人员，技能涵盖隐私与信息安全的各个方面，并拥有如 CISSP（信息系统安全认证）、CIPT（注册信息隐私技术专家）、CIPM（注册信息隐私管理师）等专业资质认证。凭借与各行业客户的广泛深入合作，我们的咨询顾问得以充分理解不同行业的合规要点并分享行业最佳实践，为企业分享独到见解与行业最佳实践，成为企业隐私合规工作的补充有生力量。

智能技术工具

Privacy Ready 的个人信息保护合规测评、管理机制，企业可获得一站式的隐私合规闭环管理体验：打通企业隐私合规管理流程，形成可复用的合规评估程序；合规问题辅助判断，力求评估结果客观、精准、可追溯；直观呈现企业个人信息保护全景视图，掌握个人信息的流通链路，实现公司层面的隐私合规标准化管理。

给客户带来的价值

- 按客户需求定制咨询服务，助力企业识别并管控风险
- 普华永道隐私合规专家智库支持，突破人才困境
- 基于亚马逊云科技的安全基础服务架构，保障数据合规安全
- 借由数字化工具 Privacy Ready，优化隐私合规流程，提升管理效率

适用行业

零售　汽车　医药　银行　其他

适用场景

个人信息保护合规；个人信息影响评估；数据分级与分类；数据全生命周期管理；数据泄露、滥用事件处置；个人信息保护合规审计；个人信息跨境传输。

联系方式

Privacy Ready 产品相关问询，请发送至：privacyready@cn.pwc.com，或联系我们的团队。

黄思维　普华永道中国网络安全和隐私服务合伙人
Tel：+86 (21) 2323 2605
Email：miles.huang@cn.pwc.com

武文俐　普华永道中国网络安全和隐私服务高级经理
Tel：+86 (21) 2323 7430
Email：janet.wu@cn.pwc.com

徐静　普华永道中国网络安全和隐私服务经理
Tel：+86 (21) 2323 6351
Email：annie.xj.xu@cn.pwc.com

普华永道举报和道德平台解决方案

应用场景

举报和道德平台(PwC's Whistleblower and Ethics Platform)是一个托管于亚马逊云科技云上的内部举报线上解决方案，平台覆盖了内部举报案件的申请、受理、处理全流程管理，并提供了相关信息资料的保存和归档功能。该平台优化了传统的举报渠道，转变企业内传统举报文化，鼓励员工及相关第三方自由地表达意见并寻求建议。

痛点及需求

企业面临的问题：

- 保护机制不健全，知情人直接面向上级汇报，举报被部门内部消化
- 传统举报沟通渠道不清晰，知情人不了解举报流程
- 数据保护法规提出更高的数据跨境传输管理和数据安全要求
- 线下管理举报案件效率较低，亟需平台化管理

后疫情时代的挑战：

- 新冠疫情导致业务模式发生变化，业务渠道及第三方服务商数量激增，企业需要覆盖面更广的数字化工具
- 线下管理举报案件，面临文档管理和归档的困难

方案优势和客户价值

普华永道一站式举报和道德平台是部署在云端的多语种举报平台，可帮助企业快速高效地在全球范围内建立内部举报受理与反馈渠道。

易用性

举报和道德平台的用户操作界面简单易懂，支持与举报人线上沟通等基础功能，同时也支持上传多种格式的文件作为举报线索。

灵活性

举报和道德平台可根据用户用量进行平台配置，实现快速登录，用户无需在本地安装软件，节约技术成本，并且 7×24 小时不间断接收内部举报，节约运营成本。

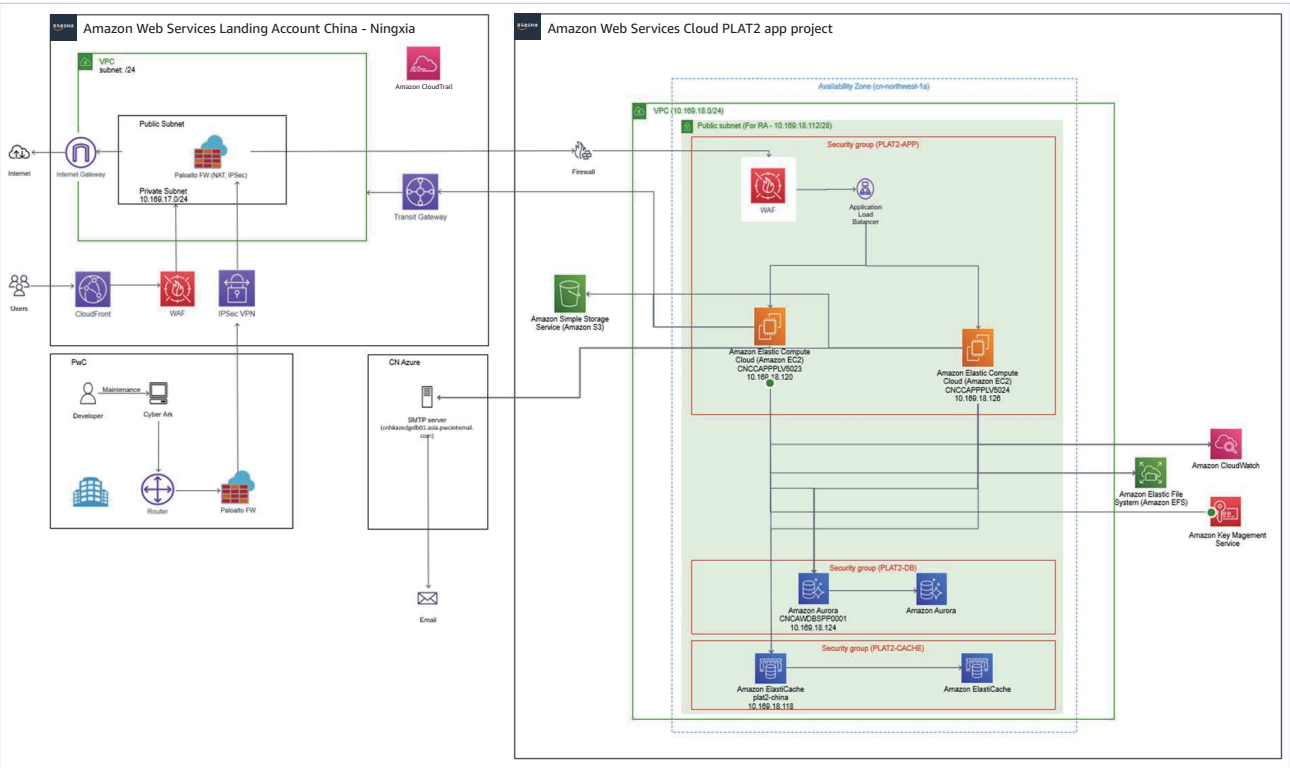
安全性

举报和道德平台严格遵守当地法律法规要求，提供严格的安全措施及定期漏洞检查，提供动态验证等登录控制功能。

全球性

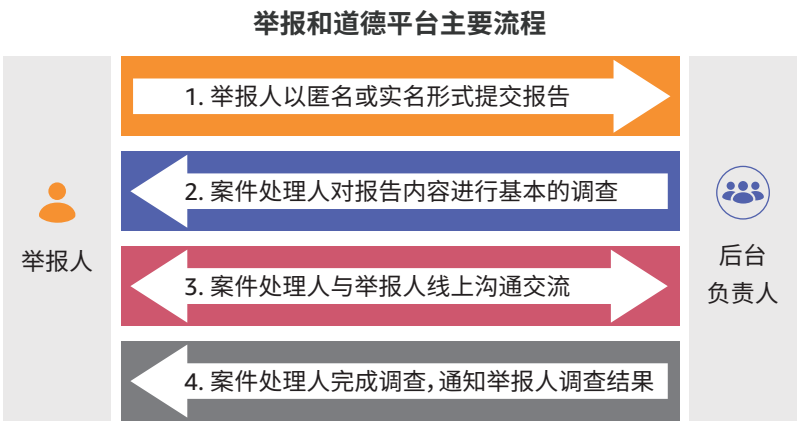
举报和道德平台支持多语种模式（中/日/英），举报人可在任何地点通过互联网提交报告，同时普华永道也会提供国际网络和专业服务支持。

架构图



方案实现方式

举报流程设计兼顾安全性及透明性，使举报人及企业后台处理人员更高效便捷地使用该平台。



举报人在举报填写时可以自行选择匿名或者实名举报，若举报人选择了匿名举报，则无需填写任何个人信息即可提交报告。

在系统层面，通过自动监测非法访问以及定期执行漏洞测试进行安全控制。在应用层面，采取动态验证等登录控制来保护系统接收到的举报信息和举报人安全。

亚马逊云科技相关服务

和本方案相关的亚马逊云科技主要服务如下：

Amazon Elastic Compute Cloud | Amazon ElastiCache | Amazon CloudTrail | Amazon Aurora | Amazon Elastic File System | Amazon CloudWatch | Amazon Simple Storage Service

叶瑜雯 普华永道中国风险及控制服务合伙人

Tel: +86 (21) 2323 7873

Email: jamie.ye@cn.pwc.com

GSI 全球行

亚马逊云科技

亚马逊云科技: aws.amazon.com

亚马逊云科技 Blog: blog.csdn.net/awschina

亚马逊云科技 Weibo: weibo.com/amazonaws

合作伙伴解决方案查找器: https://aws.amazon.com/cn/partners/find/?nc2=h_ql_pa

亚马逊云科技官方微信

亚马逊云科技官方微博

注册成为亚马逊云科技 APN 合作伙伴