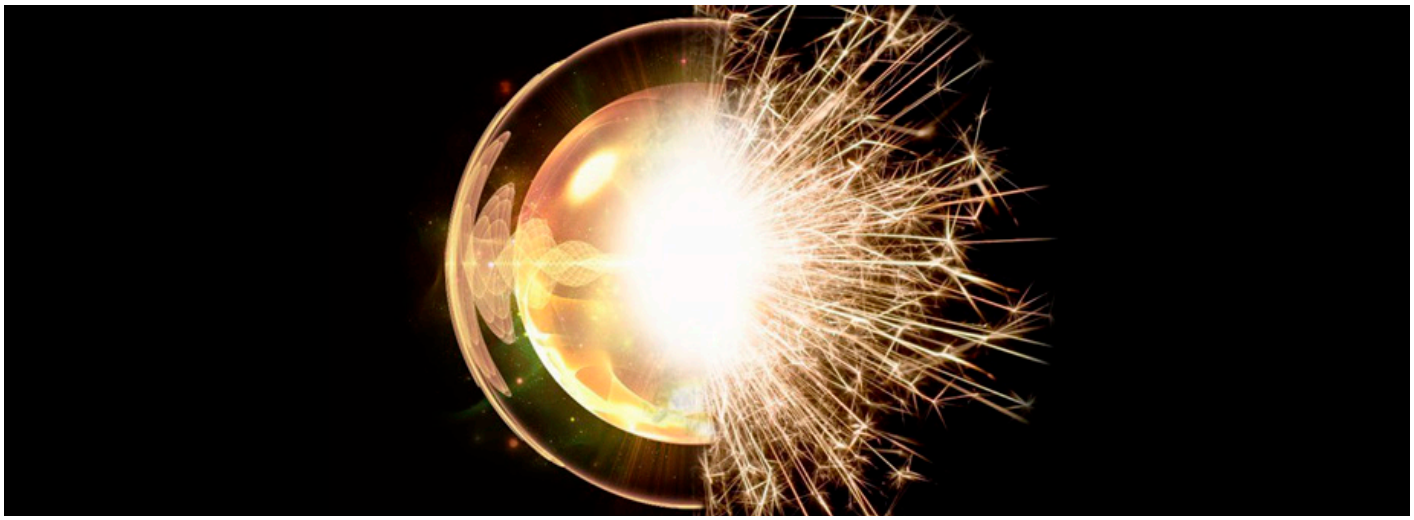
Deloitte.

德勤



扫清障碍，加速AWS部署

处理客户控制责任相关网络风险

AWS的网络风险能力

Amazon Web Services（AWS）专注于创新服务，其中包括各类公共云服务。其服务具有可扩展、弹性和灵活的特点，对企业大有裨益。作为数字化转型的主要赋能者，AWS持续推动云技术快速应用于众多行业和领域。各企业在采用云技术进行数字化转型的同时，其网络风险管理亦应顺势而变。

德勤的安全加固、预警及监控和响应及恢复（Secure.Vigilant.Resilient.™）框架内置AWS原生服务，可助力企业部署云迁移，并解决相关网络风险。

同历次重大技术变革一样，云技术一方面促进了业务创新，另一方面也促使企业掌握新的技术能力并管理网络风险。云环境不仅需要新的技术能力，还要求对既有操作模式进行重塑。

例如，现行领先的实践是自动修补源VM配置并重新加载镜像，而非事后才做补丁修复。企业在使用AWS服务的同时需承担与之相关的客户控制责任。需承担的责任取决于所使用的具体服务，不同的服务对企业的影响是不一样的。

网络安全的推进亟需加入由云创新所赋能的各类增强型安全功能。传统的强制执行和基于边界的IT防御方案已不足以应对新的风险。首席信息安全官们应顺势而为，通过增强企业现有安全能力，并使之与AWS云有机结合，以此为企业赋能。例如，可根据企业自身风险偏好、控制责任和具体的AWS云用例，在其安全战略路线图中加入相应的定制功能。

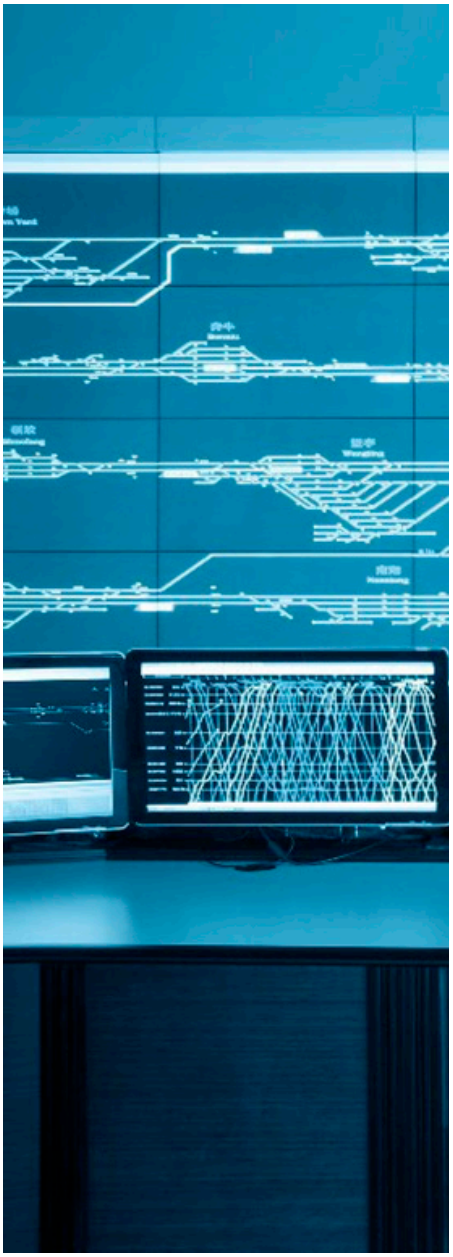
具体可加入的AWS原生安全功能有AWS Macie、AWS Trusted Advisor、AWS GuardDuty等。

通过对内部安全技术加以扩展并与AWS集成，可充分利用企业现有技术能力（如：身份和访问管理）。此外，AWS还推出了一系列新的云安全服务，专为感知云态势所打造，企业可相应选用。从客户端/服务器到基于应用程序编程接口（API）技术和无服务计算，这一跨越意味着用于解决网络风险的工具和技术应随之更新。要想云部署和安全运维齐头并进，企业必须在DevSecOps、持续集成和持续交付（CI/CD）以及协调功能方面实现安全控制自动化。

> “到2022年，至少95%的云安全故障会是客户过失所致。”[1]

1 “Is the Cloud Secure?”, Gartner, Inc., March 27, 2018, https://www.gartner.com/smarterwithgartner/is-the-cloud-secure/

云所涉及的网络风险真的有所不同吗?



责任共担模式简介

云所涉及的基础网络风险没有差别，但责任划分却大有不同。企业若自行运营数据中心，那么就应对虚拟层软件和底层基础设施的完整性负责。如果企业选择AWS云，这一责任将转由AWS承担。相反，如果选择应用程序服务提供商（ASP），再将应用程序迁移到云端，那么修补和监控应用程序的责任将由企业承担。

德勤的云服务责任共担模式定义了企业和云服务提供商各自的安全控制责任。该模式有助于阐明AWS对基础设施即服务（IaaS）和平台即服务（PaaS）相关控制域所需承担的责任。

云安全

AWS需负责AWS云的可靠性、安全性和合规性，包括对虚拟层软件和底层基础设施的完整性负责。AWS云服务运行所需硬件、软件、网络和设备统称基础设施。[2]

企业云安全部署

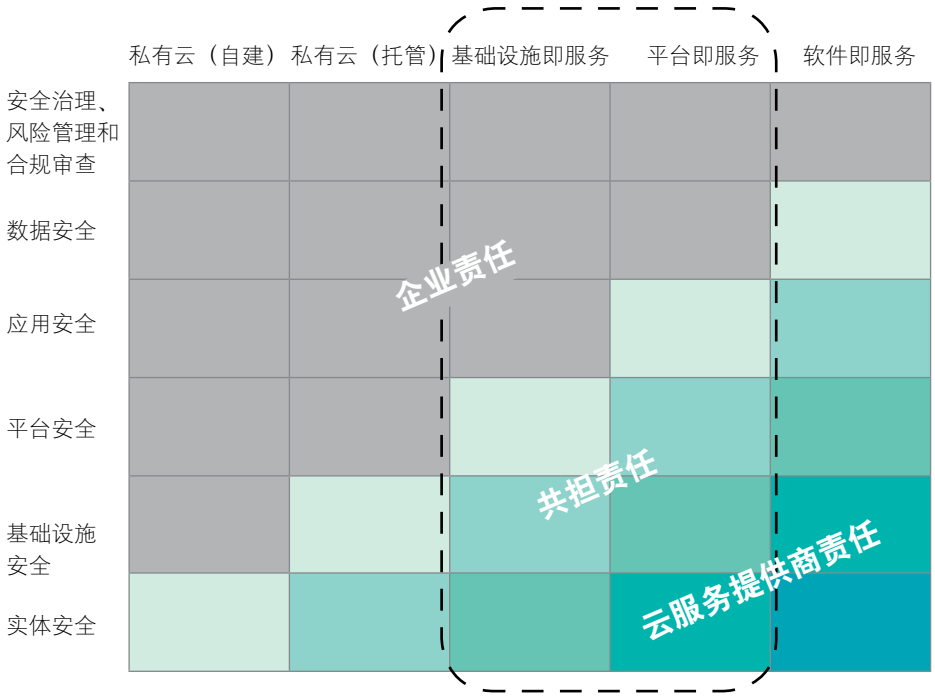
企业需要了解所选用AWS云的具体配置和与之对应的虚拟组件，并据此实施安全控制以保护自身AWS云环境。例如，如果部署了Amazon Elastics Compute Cloud （Amazon EC2）实例，企业就需负责管理客户机操作系统及已安装的应用程序软件或实用工具，并负责对AWS各项功能进行配置（如：与各实例相关的安全组）。

企业在确定其网络风险责任时，还应考虑云端数据的敏感性及自身所处的监管环境。

例如，企业应该根据自身安全政策和监管要求选择相应的加密和密钥管理模式。AWS提供多种密钥管理方案，但是企业应该选定并执行适合自身情况的首选方案。

AWS的安全行动

为维护安全、遵守法规要求及履行承诺责任，AWS在多个司法管辖区针对不同行业发起了一系列保证计划，旨在适时通知并帮助其客户。这些保证计划会对AWS服务是否符合相关法律法规进行分析并将分析情况向客户通报。此外，AWS Artifact计划引入中国，客户可通过AWS Artifact访问AWS安全与合规报告以及特定网络安全协议。



德勤的云服务责任共担模式

2 “Shared Responsibility Model”, AWS, https://aws.amazon.com/compliance/shared-responsibility-model/

AWS Artifact中可用的报告有：服务组织控制（SOC）报告、支付卡行业（PCI）报告、各辖区认证机构的认证文件以及合规报告（报告参照相关法规对AWS安全控制的实施和运行有效性进行比对）。

为管理客户责任相关风险设定基线

德勤领先助力客户应对从战略规划到实施期间所面临的各种挑战，服务涵盖云、移动、社交和分析技术。德勤通过创立安全加固、预警及监控和响应及恢复框架，借助全方位的网络风险能力和工具，并与AWS原生服务相结合，为客户提供预防性、探测性和纠正性控制措施。依托上述框架所开发的AWS网络风险管理框架不仅在安全视角及良好架构方面与AWS云部署相一致，还参照行业特定的安全与合规框架和德勤网络风险经验，对相关领先实践加以借鉴，赋能客户应对端到端的云网络风险，并综合考虑隐私、安全、监控、事件响应和治理，实现客户企业AWS云的全面整合。德勤AWS网络风险管理框架共涵盖七个网络风险领域。

德勤安全加固、预警及监控和响应及恢复框架中的安全加固提供数据丢失防护、设备加固、身份和访问管理（IAM）以及网络和基础设施安全等功能。

安全加固的核心内容，也即第一领域是网络和基础设施安全，包括虚拟基础设施，重点是保护网络信息传输、端点加固和使用AWS Shield和Web应用防火墙（WAF）来保护AWS云。作为第二领域的IAM是安全加固的另一核心。IAM旨在解决身份验证、授权、访问管理和责任追溯等各种需求。具体的构成要素包括多因素身份验证、特权访问管理和访问认证。

商业级云平台的一个基本要求是包含多层防护的安全设计，以此抵御潜在的网络攻击。采用多种技术安全控制措施以加强和保护集成平台上的AWS原生服务。第三领域是数据保护，亦属安全加固，涵盖用于保护静止状态、传输状态和使用状态数据的控制措施。其核心要素是使用AWS密钥管理服务（KMS）、CloudHSM和AWS证书管理器（ACM）进行加密、密钥和证书管理。

预警及监控包括整合本地事件源和AWS源，使安全团队能够使用情景信息更有效地识别、探测和响应安全威胁。第四领域，即日志记录和监控，涉及采用相关技术探测安全事件、对各日志源数据进行整理，并与安全信息和事件监测（SIEM）整合以监控AWS云，使企业能够确定关键数据资产的位置、访问者以及使用方式。

预警及监控的建立需要对虚拟云基础设施进行安全监控、管理临时资产并整合威胁情报。还需要利用如AWS CloudTrail、Amazon CloudWatch、AWS Lambda、Amazon GuardDuty，并通过SIEM发布AWS云态势感知警报。

第五领域，也是唯一归属响应及恢复之下的要件，包括为获取“始终在线”能力的弹性设计，以及针对应急规划、恢复能力和韧性的新模型。随着云计算成为核心业务运营所不可或缺的一部分，将由于中断而导致的宕机时间从分减少到秒很有必要。为此AWS提供了相应的功能供企业使用，如可扩展的、按需访问的API，允许企业以较低成本有效创建低时延的备用基础设施和备份，从而减少中断。其他设计理念和工具包括跨区域复制虚拟实例、多可用区域部署以及Amazon Glacier等数据归档服务。

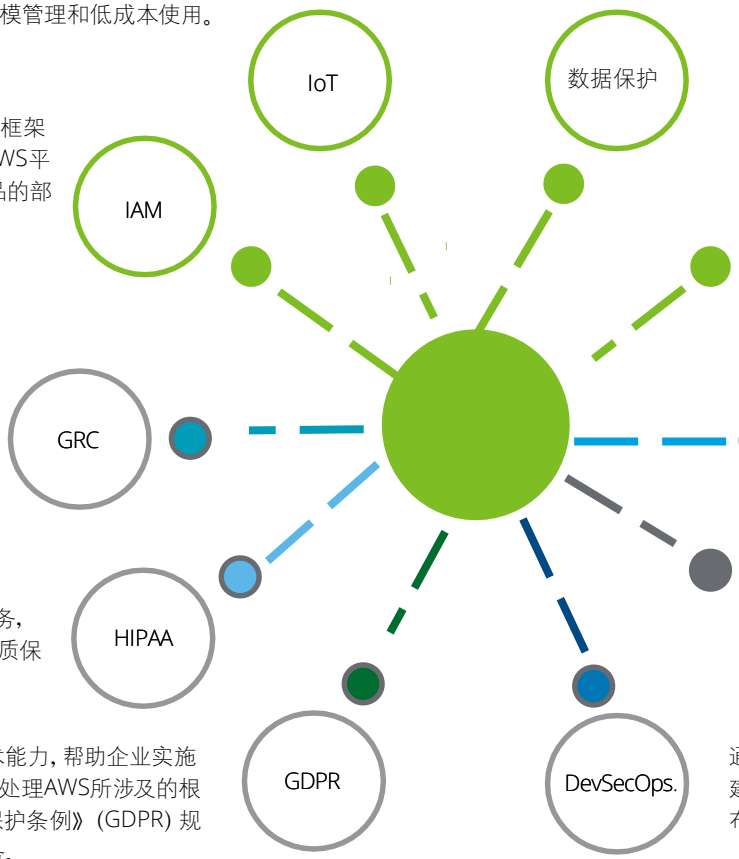
第六领域，DevSecOps，其设计包含安全加固配置、安全预警及监控和安全响应及恢复部署。上述糅合是为了使用安全软件实现业务目标。DevSecOps利用云技术的敏捷性实现安全自动化，并将其融合到DevOps流程中，用手动批准取代传统软件开发所采用的瀑布式网关。若能运用得当，DevSecOps可提高敏捷性并加快应用程序改良速度。

德勤的AWS网络风险框架提供安全能力和领先实践。第七领域，即治理、风险与合规（GRC），用于确定和管理企业特定的网络风险需求，为治理、政策、标准、流程、技术和报告的建立实施提供指引，从而实现企业目标。

德勤AWS网络风险白皮书索引

基于物联网防护 (IoT) 框架的全方位安全防御策略，旨在帮助企业建立安全优先的风险应对方案，实现大规模管理和低成本使用。

使用特定数据保护措施和原生AWS服务帮助企业保护AWS云端资产。



通过全面的IAM安全框架赋能企业有效利用AWS平台规划身份识别产品的部署和/或集成。

习如何用AWS服务和特定云工具来代替传统工具以提高基础设施的可靠性，从而减少网络攻击面。

使企业既能符合适用法规要求又能有效抵御AWS云环境下的网络风险。

利用AWS帮助客户企业提高业务连续性，改善网络风险应对方案，降低成本，提高运营效率。

提供符合《健康保险携带和责任法案》（HIPAA）规定的服务，满足行政、技术及物质保障方面的要求。

用AWS服务和第三方技术，协助企业将当前安全运维与特定云功能有效整合。

提供专业服务和技术能力，帮助企业实施适当的技术措施，并处理AWS所涉及的根据《欧盟通用数据保护条例》（GDPR）规定需履行的相关义务。

通过AWS原生DevSecOps创建连贯的部署流程以加速发布周期。

目标发布时间表

2019日历年第一季度

2019日历年第二季度

德勤和AWS

深度剖析德勤的AWS能力

德勤作为最大的网络风险专业服务机构之一，乐于将其在助力客户云转型过程中所吸取的经验教训进行分享。德勤具备广泛的网络风险能力和丰富的经验，深谙AWS原生服务，帮助各行业客户处理其在责任模型下所需承担的责任。德勤服务客户的经验写入了白皮书系列，分别归类到安全加固，预警及监控和响应及恢复框架下的各个主题。其中三篇文章讨论了与GRC、物联网、HIPAA法案和GDPR条例相关的行业特定要求；另有六篇文章提供了增强安全能力所需信息：网络和基础设施、IAM、数据保护、DevSecOps、云警戒和技术韧性。请参阅上图（“德勤AWS网络风险白皮书索引”）了解每篇文章的具体内容。

德勤网络风险服务

德勤网络风险服务业务线数十年来一直与各行业组织紧密合作。作为AWS指定的核心咨询合作伙伴，我们专精于安全工程，通过广获认可的交付方法为AWS服务，并充分利用深厚的技术经验、行业和监管知识、供应商生态系统，依托全球资深专业人士网络，帮助客户应对各类网络风险。一方面，我们为即将踏上云征程的企业制定全面战略，帮助其更好地理解和处理作为AWS客户所需承担的责任；另一方面，我们会根据具体情况执行特定功能或采用特定安全工具。我们充分利用自身在网络风险领域的广泛能力以及对AWS的深入了解为客户量身定制方案，帮助客户保护其AWS云环境，加速云部署进程，并最终实现业务成果。

战略规划与范围界定

根据具体的云服务建立特定控制措施并确立责任，创建治理模型并解决技术差距，从而减少风险

基本安全性要求；识别差距并按优先级排序，制定网络风险能力建设路线图，将其纳入AWS战略规划

实施

以德勤既有实施案例为模板为参考安全架构设定基线，建立可成功复制的方案模式和一整套安全与迭代计划

构建、测试和部署具有集成控制的安全架构；部署并记录更新的流程

优化并扩展安全能力，建立备用方案模型，确保安全运维不中断

我们助力AWS部署、应对风险和监管的价值所在

- 是AWS合作伙伴网络（APN）核心咨询合作伙伴和AWS安全能力合作伙伴（发布合作伙伴）
- 拥有云网络风险专业团队，并同AWS云安全供应商建立了合作关系
- 网络风险专业人士在使用DevSecOps设计和实现安全AWS云环境方面具有丰富经验
- 服务基于AWS技术，并利用客户能够使用的预构建集成缩短价值实现时间
- 建立了标准架构模式，可支持云态势感知、端到端的AWS安全监控解决方案
- 服务各行业领域所积累的丰富经验引导我们关注可能影响客户业务的法规、标准和网络威胁
- 在中国拥有超过200多名网络风险专业人士和 500多名技术风险专家
- 依托德勤全球成员所网络中21,000名风险管理和网络风险专业人士

德勤与AWS合作的优势

aws 合作伙伴网络

核心级
咨询合作伙伴

- 安全能力
- 政府能力
- 金融服务能力
- 公共部门合作伙伴
- MSP合作伙伴

我们的合作是将德勤在网络和企业风险管理方面的丰富经验与 AWS 安全赋能的云基础设施相结合。2006 年，AWS 开始以网络服务的形式为企业提供 IT 基础设施服务——现在俗称云计算。如今，AWS 提供十分可靠、安全、可扩展、低成本的基础设施，为全球 190 个国家 / 地区的数十万家企业提供支持，拥有超过一百万、遍布众多行业和地区的活跃客户。

德勤可以帮助企业安全地采用 AWS 并建立安全至上的云策略。作为一家领先的信息技术和咨询公司，德勤入选 AWS 合作伙伴网络（APN）核心级咨询合作伙伴和 AWS 安全能力合作伙伴（发布合作伙伴），是全球首批作为发布合作伙伴获得安全能力的八家企业之一。凭借在网络风险、AWS 和云技术方面的丰富经验，德勤能够为客户提供端到端的安全解决方案。

联系人

薛梓源
技术与网络风险咨询中国领导合伙人
德勤中国风险咨询
tonxue@deloitte.com.cn

朱昊
AWS业务主管合伙人
德勤中国管理咨询
hazhu@deloitte.com.cn

叶天斌
技术与网络风险咨询 副总监
德勤中国风险咨询
Tianye@deloitte.com.cn

柳燕
资深合作伙伴经理
Amazon Web Services
liusharo@amazon.com