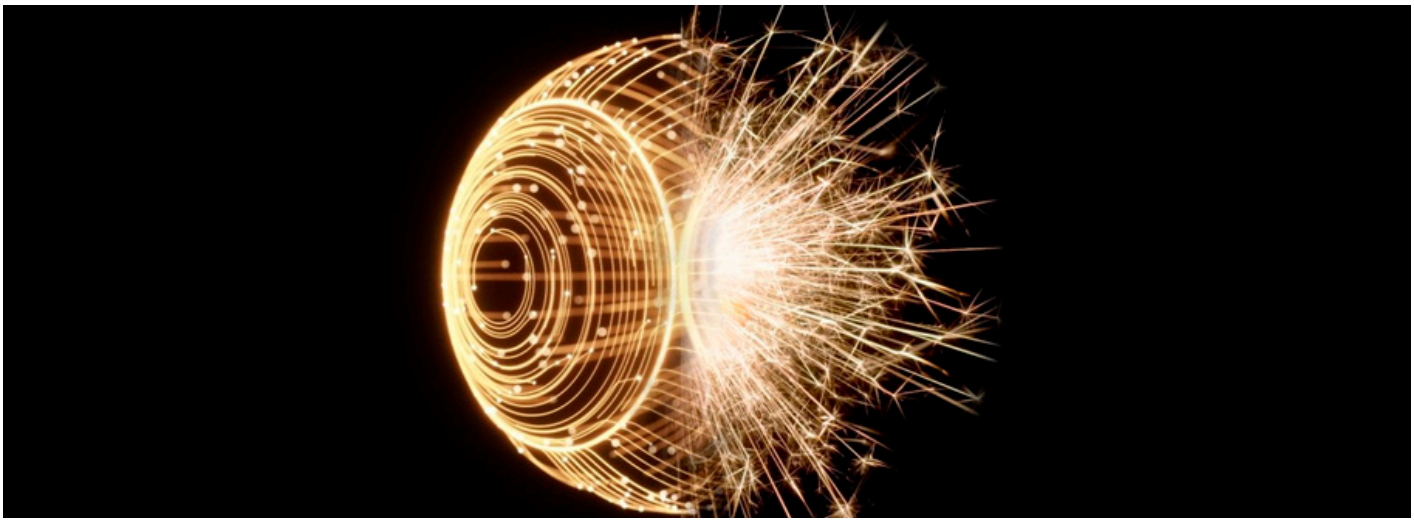
Deloitte.

aws



采用安全的云方案，扩大物联网应用

挑战

物联网技术在现代数字化世界中得到了广泛应用。智能设备和传感器能以更快的速度、更低的成本和更高的准确率收集数据并将其转化为商业洞察。许多企业已经意识到利用物联网技术推动经营决策的巨大益处，并在很多主要业务流程中融入物联网元素。

大规模采用物联网技术的企业需进行战略规划，以应对相关网络风险挑战并符合日益增多的监管要求。过去几年间，Mirai僵尸网络和震网病毒等物联网技术漏洞造成了重大的财务损失和严重的业务中断。行业领导者和业务创新者心怀

诸多顾虑，他们担心如果发生网络攻击，可能会造成投资回报率下降，影响个人生活或安全以及企业运营。因此，物联网技术的普及速度低于技术专家最初的乐观估计。这就需要构建某种能力或框架，帮助企业应对此类风险并收获高质量的投资回报。

安全性是推动企业大规模采用物联网技术的重要因素。

保护数据

德勤AWS IoT网络风险框架

为抵御这些威胁，德勤网络风险服务组利用Amazon Web Services（AWS）开发了端到端物联网安全框架，旨在帮助企业树立安全优先的意识，实现“大规模管理”和低成本技术利用。德勤在推动企业采用物联网技术的战略中直击数字网络经济最大的痛点——网络安全问题。

AWS IoT网络风险框架提供诸多方案来确保保护整个物联网堆栈的安全性。

不仅对涵盖边缘设备到后端基础设施的攻击面进行保护，还采用了纵深防御的方案。这种方案可在物联网部署的各个层面提高安全性、警惕性和韧性。[1]

该框架概述了企业应评估和实施的技术能力，以便制定可靠的安全计划，利用原生AWS服务在物联网生态系统中部署预防性、探测性和纠错性控制措施。除上述能力外，企业务必要将治理、风险和控制（GRC）能力纳入物联网生态系统。AWS服务拥有高度互操作性，可兼容客户现有的AWS云环境。

广泛部署安全能力可以有效解决物联网中一些首要的安全挑战，例如设备操作系统补丁、错误的加密机制、设备默认出厂设置、设备影子、设备事件日志、分布式拒绝服务（DDoS）攻击等。虽然这是一个相当完善的框架，但企业仍需考虑特定用例，评估是否存在其他风险和要求。

安全加固

拥有优先处理风险的控制措施以抵御已知和新兴威胁

预警及监控

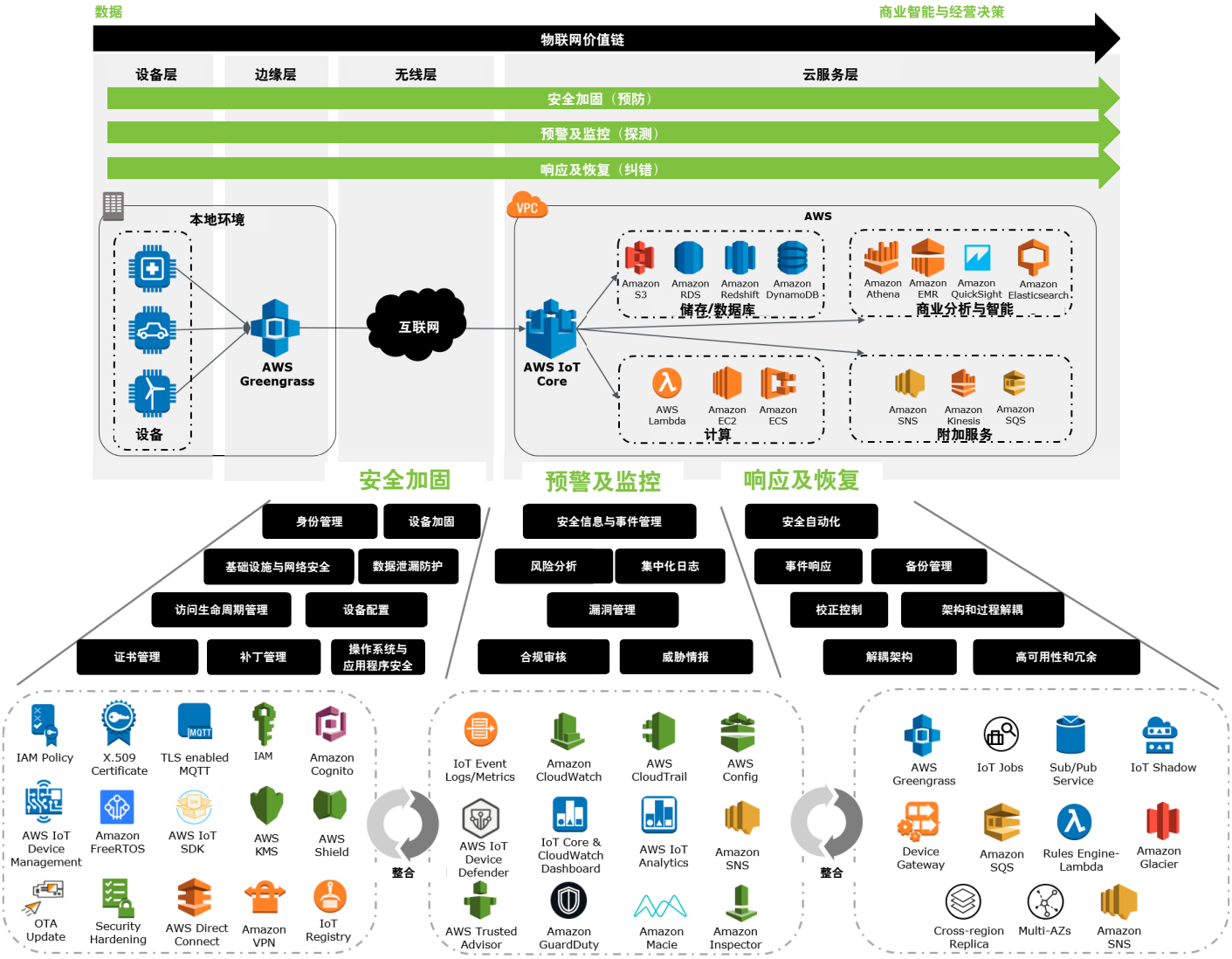
掌握威胁情报并具备态势感知能力以识别有害行为

响应及恢复

能够从网络事件中恢复并减轻相应影响

1 https://www2.deloitte.com/content/dam/Deloitte/de/Documents/risk/Risk-Cyber-Intelligence-Center-A-new-approach-to-Cyber-Security-Juni-2017.pdf

德勤物联网网络风险框架



主动保护物联网能力

要想创建构架良好的端到端安全功能，必须针对物联网基础设施制定预防性控制措施。架构师和开发人员希望打造足够稳健的基础设施来抵御潜在的网络攻击。德勤秉承领先的行业理念，再融入与不同行业的企业相关的预防性控制措施，制定出有效的安全解决方案。因此，德勤框架中的安全性支柱可提供数据丢失防护、设备安全加固、身份验证服务以及网络与基础设施安全等功能。

保护数据

物联网设备广泛应用于众多行业，存在多个独特用例。在某些情况下，设备在向上游转发数据前会执行少量加工处理；而在其他情况下，设备只是作为数据转发器。AWS IoT服务可保护这两种数据流动的安全性。

德勤框架利用AWS消息队列遥测传输（MQTT）消息代理和设备影子功能进行通信加密，通过TLS v1.2实现信息保密性。AWS IoT支持多个加密套件，允许用户使用自选的加密方法。借助行业领先实践，德勤提供依赖于原生AWS服务的高级加密功能。

锁定环境

生态系统的安全性通常取决于最薄弱的环节。在物联网中，设备/传感器布置在传统IT边界之外，用于向核心平台发送重要数据。安全应从基础细节着手，比如在连接网络前更改默认密码和用户名，以及通过系统加固程序保护设备，包括改变默认设备服务端口，如安全外壳（SSH）等。

德勤多年来提供安全服务和技术的经验显示，过时的操作系统已成为物联网的重大隐患。为此，德勤使用免费的微控制器操作系统AWS FreeRTOS来替换过时或不安全的操作系统，利用AWS服务中的免费无线（OTA）更新以实现统一的设备更新，并借助AWS IoT Device Management服务支持大规模设备管理。

德勤在资产管理方面拥有丰富的经验，可就如何安排资产维护和OTA更新提供有价值的意见。

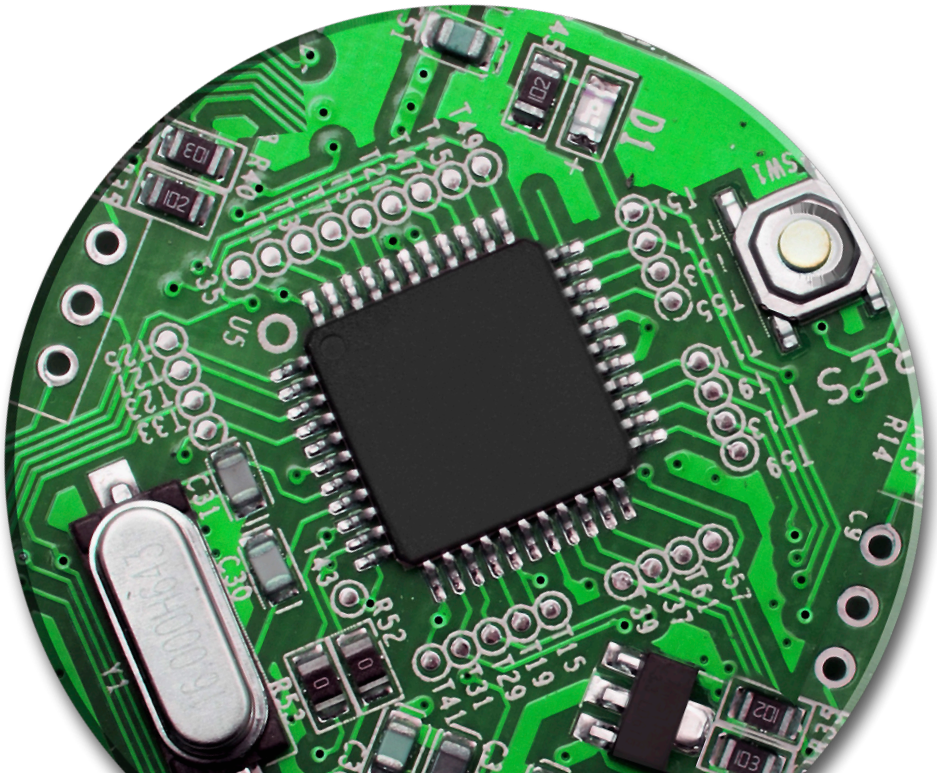
根据设备身份验证授予权限

设备若要安全连入物联网服务，需在三个主要阶段进行身份验证：（1）在访问AWS时，通过安全证书和身份验证策略进行验证；（2）当设备登录物联网平台时，使用证书和策略进行验证；（3）当物联网平台访问其他AWS服务时，通过身份角色、验证策略和安全证书进行验证。德勤运用Amazon Cognito、AWS IoT注册功能、AWS IoT Device Management、联合身份验证服务等原生AWS服务创建了严密的设备生命周期管理计划。

为进一步加强设备安全性，物联网中每个设备都通过X.509证书获得唯一身份。MQTT消息代理作为媒介对所执行的操作进行身份验证和授权，为设备和物联网平台间创造单一访问点。德勤建议主要使用AWS IoT证书，因为这样能减少操作安全支出，简化证书管理。

适当分配设备和平台通信量

AWS IoT服务使用位于边缘的安全公共端点。使用AWS Shield（一种公共端点DDoS防护服务）可进一步增强设备安全性。利用AWS IoT Core服务创建设备时，AWS根据设备使用标记和设备影子属性（又称设备孪生元），例如灯泡和发动机，对设备进行分类。每个设备类型包括多个关联，拥有唯一的设备名称和定义属性。德勤框架利用这些原生功能为设备端点提供纵深防御。此外，虚拟网络分段通过虚拟专用网（VPN）、安全组（Security Group）和网络访问控制列表（NACL）等，为AWS云中的通信提供额外一层保护。



监控与预警，毫不松懈

保护物联网基础设施的配置是部署物联网能力的第一步，亦是非常关键的一步，但企业需同等重视高级探测能力，以便快速识别环境中的异常活动。德勤的预警服务整合了本地和AWS的数据源，为安全团队提供情景信息，用以更高效地识别、探测和应对物联网设备引起的安全威胁。使用从设备层到云服务层的安全功能，包括集中化日志、威胁情报和监控，创建真正的预警环境。

收集情报，追踪设备状态

获取日志并进行集中化处理有助于企业真正保持警惕性。在物联网世界中，这些日志遍布各个平台，从设备级系统，到AWS基础设施级审核、数据访问、网络，最后到物联网特定的传输和聚合日志。3德勤的物联网网络风险框架使用AWS服务提供的日志遥测技术，通过将日志整合至单一安全的Amazon Simple Storage Service（Amazon S3）存储桶（与第三方服务配合使用），或者使用Amazon CloudWatch整合控制面板，集中处理本地日志。此外，还务必考虑AWS生态系统外部的日志源，以获得全面的安全监控方法。CloudWatch还具备原生预警功能，一旦满足某些条件即可设置阈值或标记。可靠的日志功能能够利用部署的安全事故和事件管理（SIEM）系统，实现有效的事件关联和取证。

了解并学习各项活动的影响

使用SIEM工具和服务开展威胁情报工作，非常有益于推断事件序列之间的关系并最终将相同序列归类为恶意活动。这种归类提供了具备可操作性的情报，使企业能够主动防范威胁。此外，德勤运用网络风险分析技术识别可能造成重大影响的威胁，便于企业迅速集中精力保护网络环境的关键和脆弱部分。

德勤利用原生AWS服务和第三方安全资产开发了威胁情报功能套件，为AWS IoT堆栈提供广泛的威胁情报。德勤使用的部分服务包括：

观察行为并及时响应

AWS探测服务能够将探测结果发送至Amazon CloudWatch Events。这一工具使用AWS Lambda（作为德勤韧性程序的一部分）提供自定义补救功能，并通过已经存在的企业事件管理工作流或Amazon Simple Notification Service（Amazon SNS）向管理层发出邮件或信息提醒。德勤已创建定制的Amazon CloudWatch控制面板，将AWS资源的相关指标集中在同一控制面板中，以实时显示操作状态并快速识别问题。

德勤的物联网网络风险框架利用威胁探测服务的探测结果，创建控制面板对企业内部政策和监管标准合规性进行评估，从而创造更大价值。这有利于了解AWS资源的配置，并根据所需的配置评估资源配置变更。

实现无宕机复原力

物联网市场在未来几年内可能出现巨大增长，AWS已率先开发相应服务，从安全和自动化角度管理一系列互联设备——这是确保韧性的基础。德勤与AWS持续合作，充分挖掘AWS自动化服务在设计和管理大量可扩展的安全系统方面的全部潜力。

AWS提供许多服务来应对影响韧性的核心安全能力，包括解耦架构、高可用性、冗余和安全自动化。

解耦关键任务和长期流程

亚马逊的核心订阅/发布消息收发服务——Amazon SNS和Amazon Simple Queue Service（Amazon SQS）——持续提供易于扩展和可容错的计算能力。这些工具能够实现异步的服务到服务通信，为整个网络中的分布式应用程序端点（例如订阅人）提供事件通知。订阅/发布模型具备灵活性，可根据业务需求启动不同的物联网用例，并作为业务逻辑触发规则，触发与应用或服务的下游集成。端点可在接受消息后并行工作以激活流程或缓冲队列中的任务。考虑到数以百万计的设备会生成数十亿个请求，这种解耦对于确保有效的物联网能力至关重要。

支持数据恢复

德勤框架旨在帮助创建韧性网络，能够通过持续备份重要且不可替代的数据来应对突发事件。

随着云计算应用到业务操作中，企业应转向“始终在线”的韧性模式，将中断导致的宕机时间从数分钟减少到数秒钟。AWS为企业提供必要的基础设施，以便在发生外部中断时，以跨区域复制虚拟实例、多个可用区域部署、数据归档服务（例如Amazon Simple Storage Service Glacier，简称Amazon S3 Glacier）的形式建立低延迟备份。随着物联网的兴起，AWS也在采取措施保护物联网设备的安全。德勤吸取经验——利用AWS IoT Device Gateway和AWS IoT Shadow等服务管理需要持续安全守护的指数级设备扩张。

构建韧性网络不能仅关注设备这一细小层面，还要考虑AWS生态系统并开展响应工作，以实现高可用性、冗余和低延迟云操作，从而推动建设可经受网络攻击且对业务影响最小的网络。

安排AWS机器人完成工作

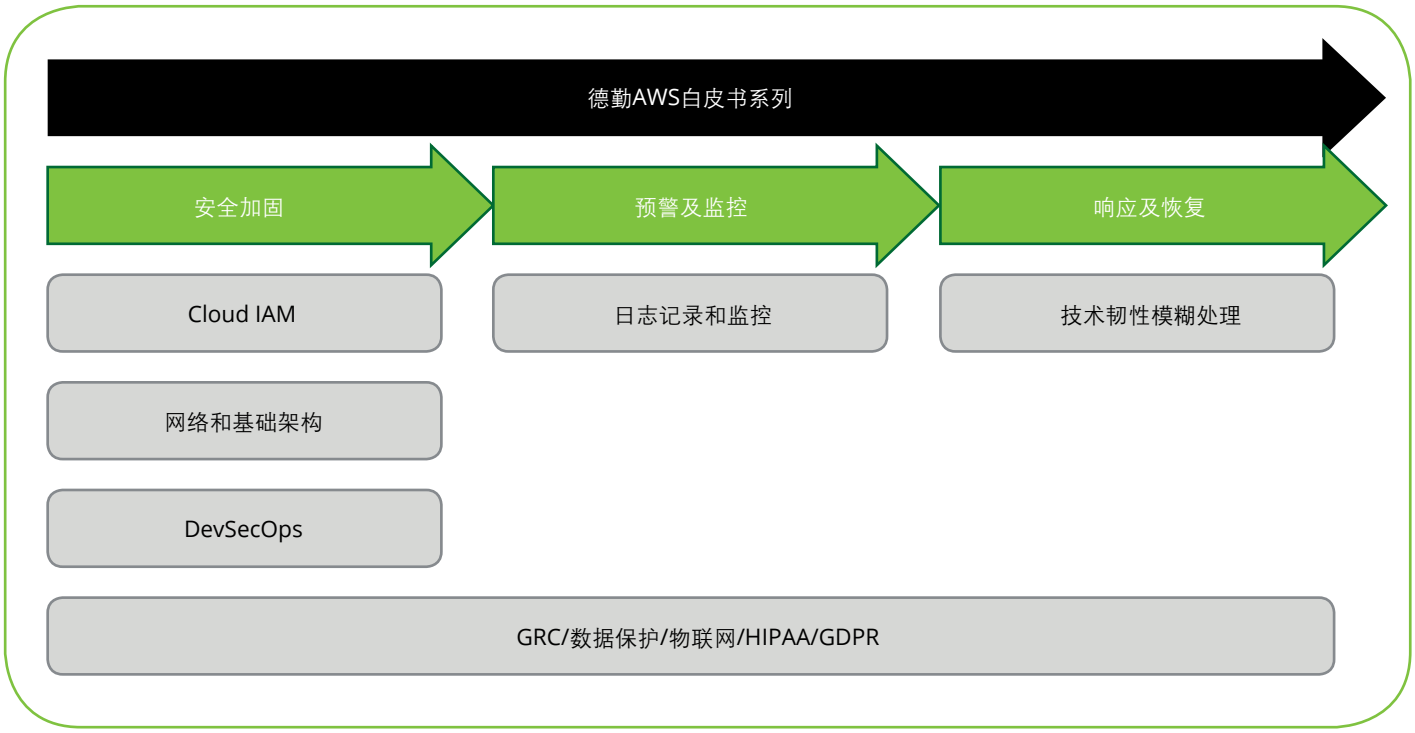
为构建和维护韧性网络及最新的安全补丁，必须实施监控。德勤利用多种AWS自动化服务持续监控资源安全性和补丁安全漏洞。AWS通过AWS Lambda、AWS IoT Greengrass和IoT Jobs等服务，推动在本地实现物联网设备安全自动化。

借助AWS System Manager等服务，德勤掌握了在AWS IoT生态系统中配置自动化安全活动的相关工具和经验。监控功能能够基于预定义规则和指定物联网操作触发自动校正，从而自动提高安全性。

2 https://docs.aws.amazon.com/iot/latest/developerguide/iot-security-identity.html#transport-security

德勤与AWS合作的优势

利用**安全加固、预警及监控和响应及恢复**（Secure.Vililant.Resilient.™）框架，再辅以AWS安全能力，德勤编制了一系列白皮书，涵盖关键的网络风险领域，着眼于解决各行业的首要AWS安全问题。



安全加固：实施可优先处理风险的控制措施，以符合监管要求并保护资产免受已知和潜在威胁的影响；
预警及监控：支持建立监控和情报方案，使企业能够识别和应对未经批准的活动，无论是无意还是恶意的；
响应及恢复：能够做好一定程度的准备，以降低事件影响并支持操作恢复。

制定计划，**立刻行动**！

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