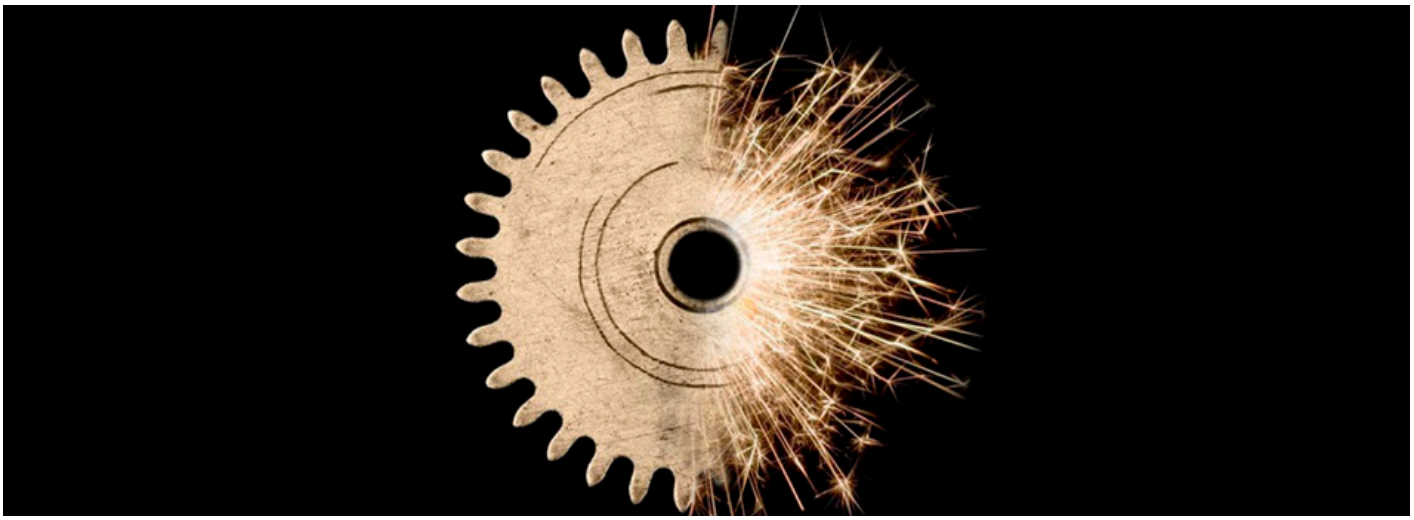
Deloitte.

aws



数据保护

保护云端数据

数据至上

采用云平台虽然可以带来可扩展性和成本节约等诸多益处，但也会让客户承担安全责任。在将工作负载迁移或部署到公共云时，企业在很多层面上最关注的一个首要问题就是安全性。企业希望确信数据受到保护。若能有效保护数据，云安全可以满足甚至超越传统环境标准。

Amazon Web Services（AWS）具有IT操作更易执行的优势，但也存在不足，一旦出现问题，错误可能会像滚雪球般不断扩大。例如，数据存储配置错误可能会暴露个人身份信息（PII）、支付卡行业（PCI）数据或受保护的健康信息（PHI）等敏感信息。最近，一家营销分析公司由于未在AWS环境中对Amazon Simple Storage Service（Amazon S3）存储桶部署适当的控制措施，导致1.23亿户美国家庭的住址、职业、房贷等信息遭到泄露。

保证云环境安全性，可以保护数据，降低这类安全事件发生的可能性。

纵深防御安全解决方案可以覆盖端到端云基础设施。德勤的安全加固、预警及监控和响应及恢复（Secure.Vigilant.Resilient.™）框架与原生AWS服务相结合，可以提供广泛的解决方案。

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。

保护数据

与传统的本地实施不同，在公共云应用中，由于云服务提供商和企业共同承担责任，需要采用不同的思维模式进行数据保护。在传统模式中，企业可以完全控制从基础设施到操作系统和数据、再到应用程序的整个生态系统。而在AWS中，基础设施由AWS实施、保护和控制，客户操作系统、数据、应用程序等虚拟基础设施服务则由企业负责。

此外，在基础设施即服务（IaaS）模式中，许多以前部署在企业数据中心的产品和服务现在都可通过公共应用程序编程接口（API）接入。这些API可从公共互联网访问，极大地改变了威胁向量和风险状况。由于存在这些产品和服务不再处于企业网络边界内的感知风险，这些差异可能会带来些许不安。

德勤利用原生AWS服务和第三方服务开发安全加固、监控及预警、响应及恢复框架，并基于该框架开发了端到端的数据保护方案。通过分层部署功能，提供预防性、探测性和纠错性控制措施，从而实现纵深防御。

采用这种数据保护方法，可通过特定的数据保护措施确保企业产品和数据安全，从而保证企业的云安全。

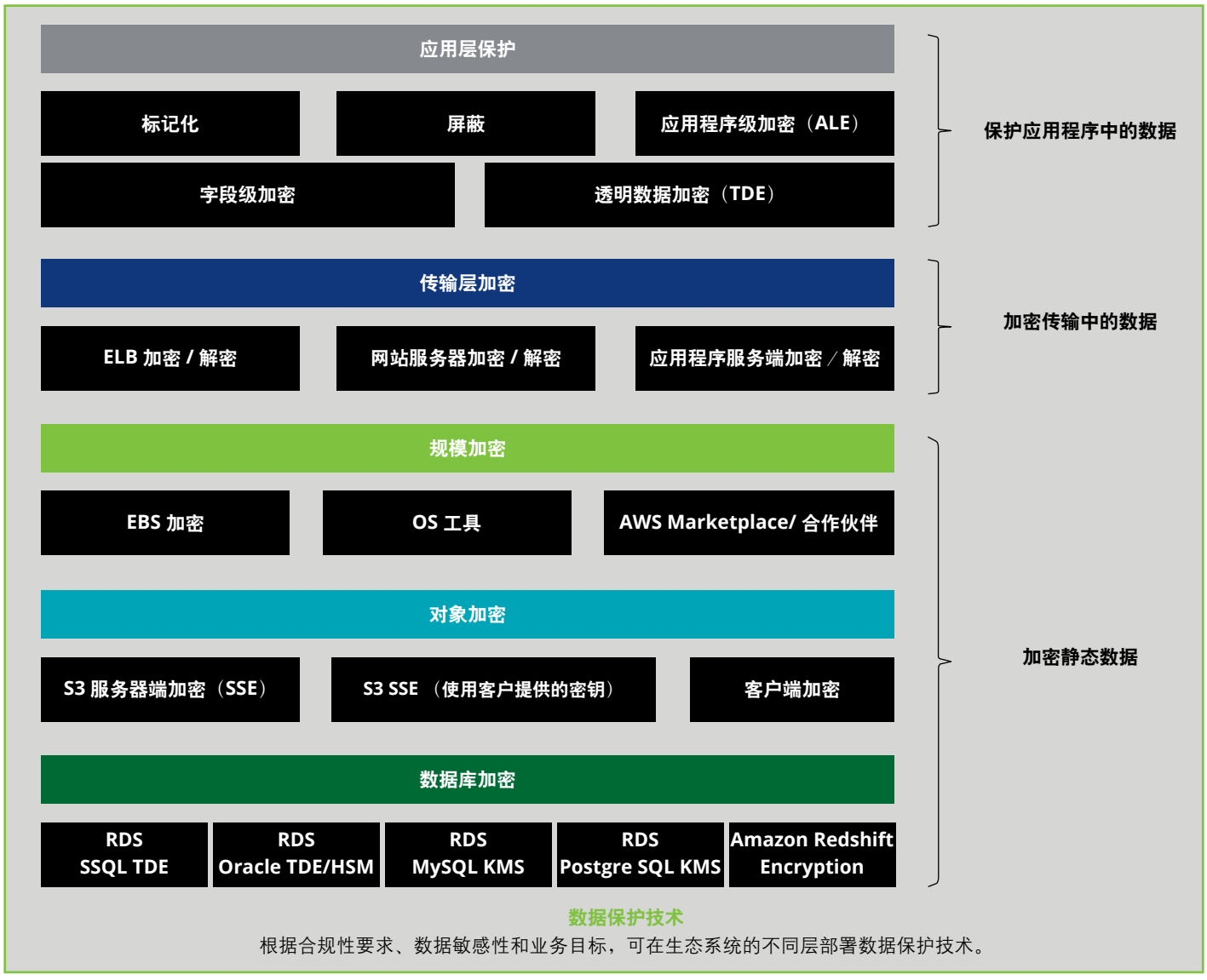
保护AWS环境

保护数据应从基础着手。在AWS环境中标记资源可使企业有效识别资源所有者并确定其中所存储数据的重要性。标记是一种经济有效的预防措施，可通过实现自动化来支持其他安全控制措施。

AWS有许多不同的存储类型，例如Amazon Elastic Block Store（EBS）、Amazon Relational Database Service（RDS）、Amazon DynamoDB和Amazon S3。每种类型都提供不同的加密选项，以保护数据免受未经授权的有意或无意访问和篡改。

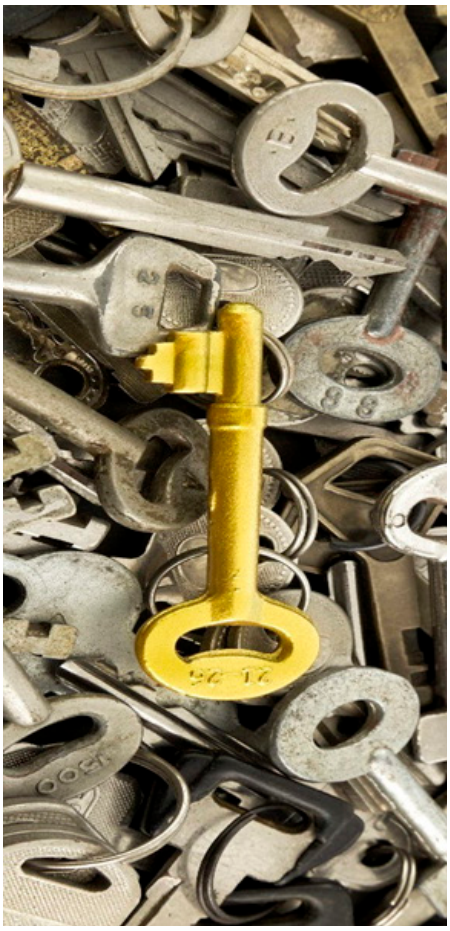
运用AWS原生加密功能是数据保护的核心要素；若结合强大的可操作密钥管理策略，则可作为一种有效的安全控制措施。

AWS生态系统中主要提供两种密钥管理服务——AWS Key Management Service（KMS）和AWS Cloud HSM（HSM），它们可以根据需求和用例独立运行或共同运行。CloudHSM为企业提供专用的物理HSM设备，该设备托管在AWS中，可由企业进行逻辑访问和管理。这样虽然增强了对加密密钥管理的控制，但CloudHSM并未直接集成其他AWS服务。而AWS KMS可使企业管理在多租户AWS HSA（Hardened Security Appliance）中生成并存储为不可导出格式的加密密钥，然后在许多AWS服务（例如，AWS CloudTrail、Amazon EBS、Amazon RDS、Amazon S3）中用于直接加密。



数据保护技术

根据合规性要求、数据敏感性和业务目标，可在生态系统的不同层部署数据保护技术。



保护AWS环境（续）

与其他一些云服务提供商不同，AWS不保留对密钥信息的访问权限，同时提供自带密钥（BYOK）选项。鉴于最近发布了CLOUD Act[1]，这一点对许多企业至关重要。对于高度敏感的工作负载，除原生AWS功能外，可能还需根据监管要求和企业风险偏好等因素使用非AWS服务提供的其他加密方法。

AWS Identity and Access Management（IAM）的安全配置策略已经提供一个强大的安全框架，通过使用细粒度角色控制对用户和应用程序的数据访问。加密则可提供第二层防御。结合IAM和密钥策略来确定对密钥操作（密钥管理和密钥使用）的访问控制，可增强环境的安全性。

除了采用CloudHSM和AWS KMS加密静态数据，还需要采用其他方案加密传输中的数据。企业可以并且应该通过使用安全的API、加密VPN隧道或AWS Direct Connect等服务，在安全通道上与AWS环境进行交互。这些方法有助于确保数据的安全传输，同时支持公共云原则。

除加密外，许多AWS工具还可用于保护云环境和数据安全。例如，AWS Secrets Manager能够自动轮换数据库凭据、API密钥和OAuth令牌等私密信息。私密信息的访问也受到IAM策略的控制。Secrets Manager是一项原生AWS解决方案，可轻松与Amazon RDS集成，从而将私密信息保存在AWS环境中，并牢牢掌控数据访问权限。

1 "S.2383 - CLOUD Act". United States Congress. February 6, 2018.

监控及预警，时刻准备就绪

保护企业数据需要掌握威胁情报并了解企业的AWS环境。因此，企业不仅要全面监控AWS环境中的资源，还要获得异常和可疑操作警报。

通过结合可用的加密和IAM功能，AWS提供原生监控机制：使用AWS CloudTrail、Amazon CloudWatch、AWS Config等服务，监控API调用、Amazon S3存储桶访问请求、加密密钥使用情况以及其他可审计事件。将这些日志源与威胁检测和恶意行为监控功能（如Amazon GuardDuty）相结合，可使企业以具有成本效率的方式了解正被访问的数据及其访问者。使用第三方安全信息与事件管理（SIEM）产品，还可以实现更高级的分析功能。

SIEM捕获的信息是威胁情报的一个主要部分，有助于检测恶意活动和可能导致数据泄露的环境配置错误。将敏感信息存储在公共Amazon S3存储桶中特别常见，这就很好地说明了为何应该进行监控以便在数据泄漏之前检测配置错误。

企业可以利用Amazon Macie来提高警报效率。Macie通过机器学习发现和分类业务关键数据，并分析访问模式和用户行为。SIEM可能会对帐户中的任何恶意活动发出警报，而Macie会对企业数据进行解读和归类，从而针对业务关键数据发出警报。

Macie的功能非常广泛，可以帮助制定非常有效的数据保护解决方案。这些功能包括使用自然语言处理来理解所存储的数据。此外，将Macie与GuardDuty结合使用，可在风险系数较高的客户数据（如帐户凭据）离开保护区域时发出警报。Macie还可以选择性地发出警报；通过机器学习了解哪些活动构成基准，仅对偏离该标准的活动发出警报。

除了利用现有的原生AWS服务，企业还可基于已识别的风险部署Cloud Access Security Broker（CASB）。CASB解决方案提供多种支持数据保护的功能，包括数据泄漏防护（DLP）、自动数据分类和支持机器学习的行为分析。这些功能能够监控数据在企业和公共云之间的传输，帮助企业阻止恶意内部人员、高级别威胁以及意外数据滥用。

杜绝中断事件：响应及恢复

数据保护不仅只是阻止其他人访问数据，更是要确保您可在需要时顺利访问数据。采用可实现数据恢复的韧性解决方案设计，是公共云数据保护的关键。

韧性设计元素可以运行快照等基础备份元素和自动VPC隔离脚本等高级技术，以限制勒索软件感染的影响。

AWS工具（如AWS Lambda）提供自定义功能以配置具体操作。例如，通过对AWS服务进行适当配置，在Amazon S3存储桶被公开时，用CloudWatch警报标记CloudTrail中捕获的审计事件，随之触发Lambda函数，以更新存储桶策略，并通过Amazon Simple Notification Service（SNS）和Amazon Simple Email Service（SES）让利益相关者了解相应情况。引言中描述的配置错误导致数据泄露的例子，可以证明这种自动化具有极高的价值。

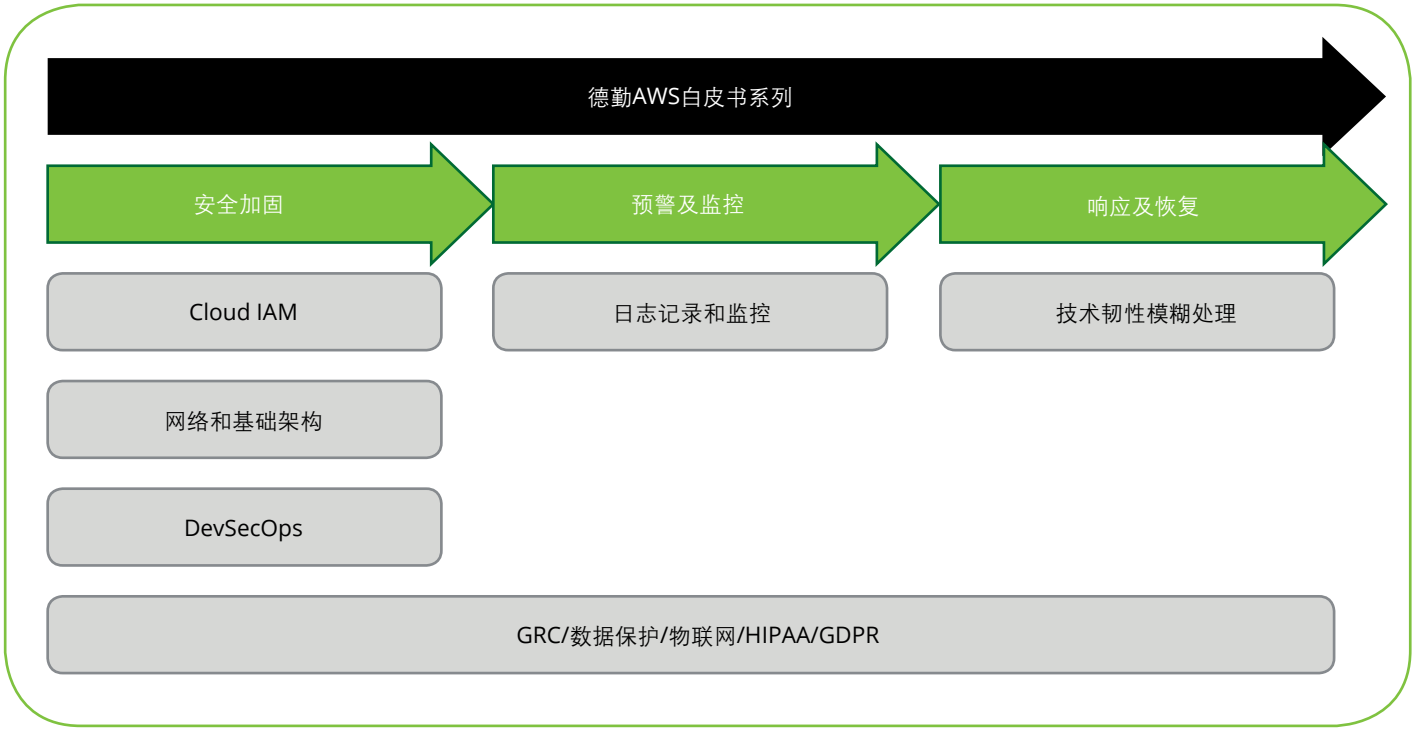
另一种利用自动化的方法是监控AWS Config规则是否合规以及IAM策略是否过于宽松，以便自动设置适当的配置和权限，避免数据丢失，同时保持应用程序性能。

结语

企业网络硬边界的概念已经逐渐消失，敏捷防御成为新的范例。数据保护是敏捷防御的核心要素，亦是保障AWS中数据和产品安全性的基石；应当全面实施数据保护，以保护传输中、静止以及使用中的数据。AWS提供大量原生服务，通过部署有效的数据保护方案，实现端到端的数据保护。凭借相关行业经验和数据保护领域知识，再结合对AWS原生功能的理解，德勤可以帮助企业利用此类功能制定最佳数据保护解决方案。

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产品免受已知和潜在威胁的影响。
预警及监控：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——无论是无意的还是恶意的。
响应及恢复：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

- 物联网分析能力
- 安全能力
- 公共部门合作伙伴
- MSP合作伙伴
- 金融服务能力

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