云计算的11类顶级威胁

关于赞助商：

新华三集团在安全领域拥有近二十年的经验积累，率先提出"主动安全"理念与技术框架，引领业界从被动防御向主动安全的理念转变。新华三拥有1200多项安全领域专利技术，近40大类超500款专业安全产品，覆盖边界安全、云安全、工控安全、数据安全、5G安全和等级保护等细分领域，具备业界最全面的安全产品和解决方案付能力，可为用户提供可信、可控的全系列网络安全产品及完整的“云-网-边-端”一体化安全解决方案。

新华三是CSA大中华区的理事单位，支持该报告内容的翻译，但不影响CSA研究内容的开发权和编辑权。

序言

随着数字经济时代的来临，云计算、大数据、5G和人工智能技术蓬勃发展，我们迎来新一轮的科技革命和产业变革。数字技术已经成为企业转型和发展的关键要素，而云是企业数字化转型的基础支柱，也是企业的首要技术重点。我国在十四五规划中，将云计算作为数字经济重点产品之首，加快数字化发展，建设数字中国，实施“上云用数赋智”行动，推动数据赋能全产业链协同转型。在数字化转型不断加深的大背景下，越来越多的企业正在将数据和应用程序迁移到云中。云上安全问题也更加广泛和突出。IDC调研显示，云计算所面临的挑战中， 安全问题排在首位。2022年RSA大会上，云安全已经成了创新沙盒最热门赛道。

历年的《云计算顶级威胁》给出了企业在使用云计算服务时面临的11类顶级威胁，并对每类威胁问题进行了分析。11类顶级威胁突出反映了当前云计算使用过程中最重要的几类云安全问题：身份和访问管理、API安全、错误配置和变更控制、以及缺乏云安全架构和策略。基于2022年威胁的排名可以发现，身份管控、API安全在云安全中的重要性明显上升，同时，云配置和变更控制依然占据很重要的位置，第三方资源（源代码、SaaS产品和API风险）的安全则是供应链安全主要关注的风险。云原生技术架构使得云计算具有了弹性、敏捷、资源池和服务化等特征，容器化和无服务器负载显著提高了云计算应用的敏捷性，但同时也带来了新的安全要求和挑战。无服务器和容器化工作负载的错误配置和利用，可能导致系统中断、数据泄露、数据丢失、以及攻击发生。

未来，云计算市场依然持续高速增长，根据IDC数据，预计2020-2025年中国云计算复合增长率达到26.3%，安全性会是企业上云、用云首要、长期关注的内容。云计算架构的不断发展使得多云、边缘云、分布式云成为了新的发展趋势，同时，云原生技术及开发流程进一步普及，容器、无服务器架构、云原生应用程序开发流程、API 等会成为越来越广泛的应用。攻击日新月异，我们也无惧挑战，云安全在向着多云安全、零信任、数据安全、云原生安全等技术发展趋势不断深入，风险面对，责任共担，大家共同携手促进云安全技术及产业生态的完善建设，护航行业数字化上云之路，开拓数字化新时代。

李雨航 Yale Li

CSA 大中华区主席兼研究院院长

目录

概要

顶级威胁报告一贯旨在提高对云威胁、漏洞和风险的认识。我们在撰写本报告前，调查了700多位业界专家并探讨了云行业的安全问题。今年，受访者评估了云环境中的11个重要安全威胁。顶级威胁工作组结合调查结果和专业知识编写了2022年度《云计算的11类顶级威胁》报告。

最新报告按调查结果重要程度着重介绍了前11类威胁（括号中的是2019年调查的排名）：

1. 身份、凭据，访问和密钥管理、特权账号管理的不足 (4)
2. 不安全的接口和API (7)
3. 配置不当和变更控制的不足 (2)
4. 缺乏云安全架构和战略 (3)
5. 不安全的软件开发
6. 不安全的第三方资源
7. 系统漏洞 (8)
8. 云计算数据的意外泄露
9. 无服务器和容器化工作负载的配置不当和利用
10. 有组织的犯罪、黑客和APT攻击 (11)
11. 云存储数据泄漏

观察和依据

2019新冠病毒大流行和随后的封锁重新定义了工作场所，居家办公不再是一种员工乐于接受的弹性工作方式，而是企业持续经营的必要条件。云工作负载、供应链以及边缘计算、物联网（IoT）、运营技术（OT）和区块链等新技术的流行和复杂性改变了云安全格局。软件定义边界（SDP）和零信任架构（ZTA）等新概念改变了我们对资源访问的看法。

我们在分析了调查的所有反馈之后，注意到在云服务提供商（CSP）的努力下，传统云安全问题的排名持续下降。2019年度《云计算的11类顶级威胁》（EE）中描述的拒绝服务、共享技术漏洞、CSP数据丢失和系统漏洞之类问题的排名现在非常低，已不在

本报告之列。这表明，人们明显加大了对云的信任；基础设施即服务（IaaS）环境中的老式云安全问题似乎不那么令人担忧。此外，我们发现数据泄露不再是首要的云安全问题。

调查中评分较高的调查项目指出云用户是薄弱环节。受访者不再关注元结构（EE中排名为9）、控制平面薄弱（EE中排名为8）或云使用可见性（EE中排名为10）是否会成为云部署中的问题。从2016年的顶级威胁（Treacherous Twelve）到2019年的顶级威胁（EE），再到今年的调查评估获得的顶级威胁，关注点不断变化。今年的顶级威胁突显了用户直接控制相关的安全问题：身份和访问管理、加密、配置管理、不良的编码习惯以及对战略云方向的忽视。敏捷项目管理和DevOps项目的上升使终端软件团队直面这些复杂的组合性问题。

表现优异的云企业将是那些强调变革管理、增加员工交叉培训、嵌入团队安全拥护者以及在文化上做到安全与合规的公司。新冠封锁的要求结束之后，云继续蓬勃发展，并成为每天的期望。本报告通过调查分析这十一种威胁、风险和漏洞，为云方向未来的成功助力。

目标读者

云和安全从业者和爱好者可以从本报告受益，了解云安全威胁和挑战的最新情况、对行业的影响，以及个人或行业可以采取的改进措施。最后，这项基于调查的研究也为合规、风险、技术人员和管理层提供了当前的技术趋势和高优先级云安全问题。

调查

在撰写2022年度《云计算的11类顶级威胁》报告时，CSA顶级威胁工作组的研究包含两个阶段。这两个阶段都调查收集了网络安全专业人员对云计算最相关的威胁、漏洞和风险安全问题的想法和意见，最终确定了2022年度的顶级威胁。

在第一个研究阶段，该小组的目标是通过对工作组成员的调查，创建一个云安全问题候选清单。工作组从一个包含26个安全问题的清单入手（2019年EE报告中的11个问题，以及通过讨论增加的15个新问题）。工作组通过一系列的会议对26个问题进行了讨论，

并要求成员们说明每个问题对其组织的重要性以及他们对自己熟悉的组织的了解。

在这个研究阶段，工作组成员们也可以提出这26个问题之外的其他问题。综合以前调研结果和其他相关信息，工作组标定了19个最突出的云安全问题。

在第二个研究阶段，工作的主要目标是通过对非工作组安全专业人员进行在线调查，按照重要性对上阶段列出的19个问题排名。调查对每个问题的重要性评估，满分为10分。调研对象按照“1至10分”对云安全问题评级打分，1分代表非常不重要，10分代表非常重要。对每个问题的得分计算平均值并行排序。排除所有低于7分的安全问题，最终得出了如下11类顶级威胁：

调查结果排名	调查平均得分	威胁名称
1	7.729927	身份、凭据，访问和密钥管理、特权账号管理的不足
2	7.592701	不安全的接口和API
3	7.424818	配置不当和变更控制的不足
4	7.408759	缺乏云安全架构和战略
5	7.275912	不安全的软件开发
6	7.214493	不安全的第三方资源
7	7.143066	系统漏洞
8	7.114659	云计算数据的意外泄露
9	7.097810	无服务器和容器化工作负载的配置不当和利用
10	7.088534	有组织的犯罪、黑客和APT攻击
11	7.085631	云存储数据泄露

工作组在确定了11类顶级威胁后，分析了每类威胁问题，描述具体威胁问题，指出了CSP或云客户是否共同承担安全责任，并定义了问题在云堆栈以及云服务模型（SaaS、PaaS、IaaS或SPI）中可能出现的位置。业务影响、关键信息、案例展示了每类威胁可能出现的情况和场合。可以通过CSA云计算关键领域安全指南（CBK）v4.0、CSA云控制矩阵（CCM）v4.0了解相关概念的推论和缓解措施，依据STRIDE威胁模型和引用链接了解案例详情。

威胁 1:

不充分的身份、凭据，访问和密钥管理、特权账号管理

身份、凭据和访问管理系统包括允许组织管理、监视和安全访问有价值资源的工具和策略。有价值资源的举例有电子文件、计算机系统和物理资源（如服务器机房和建筑物）。

适当维护和持续警惕很重要。在身份与访问管理（IAM）中使用风险评分可以增强安全态势。使用清晰的风险分配模型、仔细监控和采取适当的行为隔离可以帮助交叉检查IAM系统。跟踪目标访问和风险评分频率对于理解风险背景也至关重要。

特权账户必须以准确、即时的方式冻结，避免人员在离职或角色更换后进入。这将减少数据泄漏或受损的可能性。除了取消某些特权账户外，账号角色和职责必须符合对信息“按需所知”的程度。享有特权的人员越多，越会增加数据管理不善或账户乱用的可能性。

安全责任

- ✓ 客户
- ✗ 云服务供应商
- ✗ 共同

架构

- ✓ 应用程序
- ✓ 元数据
- ✓ 信息
- ✗ 基础设施

云服务模型

- ✓ 软件即服务 (SaaS)
- ✓ 平台即服务(PaaS)
- ✓ 基础设施即服务(IaaS)

业务影响

身份、凭据，访问和密钥管理、特权账号管理不足的负面影响可能包括：

- 由于被动和过多的限制封锁，导致业务绩效和生产力下降
- 员工测试疲劳导致不合规和对安全意识淡薄（漠不关心）
- 未经授权或恶意用户替换、未经授权或恶意用户的泄露
- 失去市场的信任和收入
- 因事件响应和取证而产生的财务费用
- 勒索软件和供应链中断

关键信息

正确的IAM、凭据和密钥管理措施可能包括：

1. 加强企业架构核心的防御，让对终端用户身份的攻击成为一种很容易实现的目标。
2. 稳健的零信任层需要采取针对零散用户的简单身份验证和基于应用程序的隔离之外的其他措施。
3. 运营政策和结构性风险模型对于CIEM等高级工具也至关重要。 [1]
4. 必须根据业务需求对用户对象进行动态风险评分。应该努力获得用户的信任，而不是简单地为其提供密钥和代码。

案例

最近的一些案例包括：

- (2021年)，出现了涉及Twitch、Cosmology Kozmetik、PeopleGIS、Premier Diagnostics、SeniorAdvisor、Reindeer和Twillo的漏洞，其中大多数攻击是属于内部威胁之一的特权滥用。不监控风险和韧性的公司面临着动态威胁。[2]
- (2021年10月) 深入了解世嘉（SEGA）欧洲的云服务器事件，就会发现有两个重要的云配置管理错误——AWS S3存储桶设为公共访问权限、硬编码凭证存储在云中。如果提交了文件到沙盒，AWS和CDN网络中的内容替换就可以避免，从而允许系统有更多时间验证更改并对访问环境进行风险评估。[3]
- (2019年1月到7月) CapitalOne银行内部违规使用AWS云事件，其中借用动态IAM角色是关键的违规行为。虽然S3 存储桶不像其他许多漏洞那样暴露在互联网上，但EC2实例有过多IAM角色可能是罪魁祸首。[4]

CSA云计算关键领域安全指南 v4.0

领域 2: 治理与企业风险管理

领域 4: 合规和审计管理

领域 5: 信息治理

领域 6: 管理平面和业务连续性

领域 11: 数据安全和加密

领域 12: 身份、授权和访问管理

领域 14: 相关技术

CSA云控制矩阵 v4.0

AIS 应用程序和接口安全

AIS-01: 应用程序和接口安全策略和规程
AIS-02: 应用程序安全基线需求
AIS-03: 应用程序安全指标

CCC 变更控制和配置管理

CCC-07: 基线偏离检测
CCC-08: 例外管理

DSP 数据安全与隐私生命周期管理

DSP-03: 数据清单
DSP-04: 数据分级分类
DSP-07: 设计和默认数据保护
DSP-17: 敏感数据保护
DSP-19: 数据位置

GRC 治理、风险管理和合规

GRC-02: 风险管理计划
GRC-05: 信息安全计划
GRC-06: 治理责任模式1

IAM 身份与访问管理

IAM-01: 身份与访问管理的策略与规程
IAM-03: 身份清单
IAM-05: 最小权限
IAM-08: 用户访问评审

LOG 日志记录和监控

LOG-10: 加密监控与报告

LVS 基础设施与虚拟化安全

IVS-03: 网络层安全

TVM 威胁和漏洞管理

TVM-08: 漏洞优先级

	Stride威胁分析	引用链接
✗	身份欺骗	1. CIEMHome-CIEM-HOME(ciemgroup.com)
✗	篡改数据	2. Worst AWS Data Breachest of 2021 https://sonraisecurity.com/blog/worst-aws-data-breaches-of-2021/
✗	抵赖	3. SEGA Europe Thoroughly Scrutinizes its Cloud Security https://vpnoverview.com/news/sega-europe-security-report/Securin Blog | Lessons Learned from SEGA Europe's recent security blunderSEGABarelyAvoidedHugeDataBreachAfterItLeftDatabasePublicly Open | Everys
✓	信息泄露	
✗	拒绝服务	4. The Capital One - AWS incident highlights the roles and responsibilities of cloud customers, providers https://diginomica.com/capital-one-aws-incident-highlights-roles-and-responsibilities-cloud-customers-providers
✗	权限提升	

威胁 2:

不安全的接口和API

API使用越来越流行，保护这些接口已变得至关重要。必须检查API和微服务是否存在由于错误配置、不良的编码习惯、缺乏身份验证和不恰当的授权而导致的漏洞。这些疏忽可能使接口容易受到恶意活动的攻击。常见例子包括：1、未经验证的端点；2、弱身份认证；3、过度的权限；4、禁用标准安全控制；5、未应用补丁的系统；6、逻辑设计问题；和7、禁用日志记录或监控。API和其他接口的错误配置是导致事件和数据泄露的主要原因，从而可能导致允许过滤、删除或修改资源、调整数据或中断服务。

安全责任	
✓ 客户	
✓ 云服务供应商	
✗ 共同	
架构	
✓ 应用程序	✓ 元数据
✓ 信息	✗ 基础设施
云服务模型	
✓ 软件即服务 (SaaS)	
✓ 平台即服务(PaaS)	
✓ 基础设施即服务(IaaS)	

组织正在快速推进（为供应商和消费者）API的使用，以提高连接性和灵活性。API的好处包括为API开发人员和客户提供数字体验。由于API的快速增长和使用，开发人员在管理和保护

API方面面临着一项具有挑战性的任务。Akamai 2021的一份报告记录了“在上一年中，Akamai交付了超过300万亿API请求，同比增长53%。”[1]各种类型的API供应商和消费者模式的复杂网络也有助于对API编目。编目API必须包括一些细节，如内部或外部API、用途、公开的数据以及API使用方式。正如API简化了数字生态系统一样，云技术也是推动快速、轻松创建或使用API的催化剂。扩展和自动化需要不同技术和云服务供应商都采取标准化的安全模式。在当前API使用指数增长的情况下，持续的监控和测试方面可能也会面临一些问题。

业务影响

不安全的接口或API的风险因API的使用和相关数据以及检测和缓解漏洞的速度而异。

最常见的业务影响是API未保护敏感或私人数据而造成意外暴露。

关键信息

以下是一些关键信息：

1. 应跟踪、配置和保护API提供的攻击面。
2. 需要更新传统的控制和变更管理策略和方法，从而跟上以云为基础的API的增长和变化。
3. 公司应该接纳自动化，并采用能够持续监控异常API流量和近实时修复问题的技术。

案例

最近的一些案例包括：

1. (2021年4月28日) 据一位安全研究人员报道，益博睿（Experian）的一家合作伙伴网站允许任何人通过提供用户姓名和邮寄地址查询数千万美国人的信用分数。虽然数据集属于信贷机构益博睿，但第三方可以获取相关服务。[2]
2. (2021年5月5日) 高档互动健身器材公司Peloton中断了用户身份验证和对象级授权，在直接调用时通过API暴露了客户的PII类型数据，包括用户ID、位置、体重、性别、年龄等。[3]
3. (2021年4月22日) 农业机械、重型设备和草坪护理设备制造商约翰迪尔（John Deere）允许任何人在没有身份验证或速率限制的情况下查询用户名。研究人员很快确定，《财富1000强》中近20%的公司拥有约翰迪尔账户。另外，还发现可以通过VIN车辆识别代码查询API接口查找显示设备所有者信息，包括地址和拖拉机名称等数据。[4]

CSA云计算关键领域安全指南 v4.0

领域 4: 合规和审计管理

领域 5: 信息治理

领域 6: 管理平面和业务连续性

领域 7: 基础设施安全

领域 8: 虚拟化和容器

领域 10: 应用安全

领域 11: 数据安全和加密

领域 12: 身份、授权和访问管理

CSA云控制矩阵 v4.0

AIS 应用程序和接口安全

AIS-01: 应用程序和接口安全策略和规程
AIS-04: 应用程序安全设计和安全开发
AIS-06: 自动化应用程序安全部署

DSP 数据安全与隐私生命周期管理

DSP-01: 安全与隐私的策略和规程
DSP-03: 数据清单
DSP-04: 数据分级分类
DSP-05: 数据流文档

CEK 密码学、加密与密钥管理

CEK-03: 数据加密
CEK-04: 加密算法

IVS 基础设施与虚拟化安全

IVS-03: 网络层安全
IVS-04: 操作系统加固与基线控制
IVS-09: 网络防御

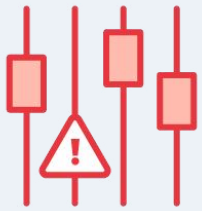
CCC 变更控制和配置管理

CCC-01: 变更管理策略和规程
CCC-02: 质量测试
CCC-05: 变更协议

	Stride威胁分析	引用链接
✗	身份欺骗	1. AkamaiReport:https://www.ir.akamai.com/static-files/1ef574a5-ae14-48f6-854a-47d96c4a75fe 2. Experian API Exposed Credit Scores of Most Americans: https://krebsonsecurity.com/2021/04/experian-api-exposed-credit-scores-of-most-americans/ 3. Peloton's Leaky API Spilled Riders' Private Data: https://threatpost.com/pelotons-spilled-riders-data/165880/ 4. LeakyJohnDeereAPI's:SeriousFoodSupplyChain Vulnerabilities:https://sick.codes/leaky-john-deere-apis-serious-food-supply-chain-vulnerabilities-discovered-by-sick-codes-kevin-kenne
✓	篡改数据	
✗	抵赖	
✓	信息泄露	
✗	拒绝服务	
✗	权限提升	

威胁 3：

配置不当和变更控制的不足



安全责任
✓ 客户
✓ 云服务供应商
✓ 共同
架构
✓ 应用程序　✓ 元数据
✓ 信息　✗ 基础设施
云服务模型
✓ 软件即服务 (SaaS)
✓ 平台即服务(PaaS)
✓ 基础设施即服务(IaaS)

配置不当是指计算资产的不正确或次优设置，可能使其容易受到意外损坏或外部/内部恶意活动。缺乏系统知识或对安全配置和恶意意图的认识可能会导致错误配置。一些常见的错误配置有：1、不安全的数据存储元素或容器；2、过度的权限；3、默认凭据和配置设置保持不变；4、禁用标准安全控制；5、未应用补丁的系统；6、日志记录或监控已禁用；7、不受限制地使用端口和服务；8、无担保的密钥管理；9、很差的配置或缺乏配置验证。云资源配置错误是导致数据泄露的主要原因，也可能导致资源删除或修改以及服务中断。

云环境中的变更控制不足可能会导致错误配置，并阻碍了纠正错误配置。云环境和云计算方法不同于传统的信息技术（IT），其方式使变化更难控制。传统的变更流程涉及多个角色和批准，因此需要几天或几周才能实现生产。云计算最佳实践依赖于自动化、角色扩展和访问支持快速变化。在企业数据中心，静态基础设施元素可以抽象为云环境中的代码。最后，由多个供应商几乎每天都在增强和扩展自己的独特功能，使用多个云供应商增加了复杂性。这种动态环境需要采取一种敏捷和主动的方法进行变更控制和补救，许多公司正试图掌握这种方法。

业务影响

根据错误配置/不当变更的性质以及检测和缓解的速度，错误配置/不当变更控制的影响可能会很严重。云审计知识证书学习指南,中的影响分类如下：

1. 数据披露-技术影响机密性
2. 数据丢失-技术影响-可用性
3. 数据破坏-技术影响-完整性
4. 系统性能-运营影响

5. 系统中断-运营影响
6. 勒索需求-财务影响
7. 违规和罚款-合规和财务影响
8. 收入损失-财务影响
9. 股价下跌-财务影响
10. 公司声誉-声誉影响

关键信息

以下是一些关键信息：

- 公司需要采用可用的技术不断扫描出配置不当的资源，以便实时修复漏洞。
- 变更管理方法必须能够反映持续和动态的业务变化和安全挑战，确保可以使用实时自动验证方法确保许可变更的正确性。

案例

最近的一些案例包括：

1. (2022年3月9日) 据报道，由于客户管理的ServiceNow ACL（访问控制列表）配置错误以及为访客授予过多权限，测试的ServiceNow实例中近70%存在安全问题。[1]
2. (2021年10月4日) Facebook拥有的应用程序Facebook、Instagram、Whatsapp和Oculus下线。配置错误的更改会中断通信，而协调数据中心之间网络流量的主干路由器会导致通信中断。网络流量的中断对数据中心的通信方式产生了级联效应，导致服务停止。此次停机还影响了日常运营中使用的许多内部工具和系统，使问题的诊断和解决变得复杂。[2]
3. (2021年1月7日) 据报道，微软错误配置了其自己的Azure Blob（云）存储桶，其中存储了第三方数据，误披露了来自希望与微软合作的公司的100多个“募资简报”和源代码，包括创意和知识产权。[3]

CSA云计算关键领域安全指南 v4.0

领域 4: 合规和审计管理

领域 5: 信息治理

领域 6: 管理平面和业务连续性

领域 7: 基础设施安全

领域 8: 虚拟化和容器

领域 10: 应用安全

领域 11: 数据安全和加密

领域 12: 身份、授权和访问管理

CSA云控制矩阵 v4.0

A&A 审计与保障

A&A-02: 独立评估
A&A-03: 基于风险的规划评估

AIS 应用程序和接口安全

AIS-02: 应用程序安全基线需求
AIS-04: 应用程序安全设计和安全开发
AIS-05: 自动化应用程序安全测试

BCR 业务连续性管理和运营韧性

BCR-02: 风险评估和影响分析
BCR-03: 业务连续性策略
BCR-08: 备份

CCC 变更控制和配置管理

CCC-02: 质量测试
CCC-04: 未经授权的变更保护
CCC-09: 变更恢复

CEK 密码学、加密与密钥管理

CEK-03: 数据加密
CEK-05: 加密变更管理

DSP 数据安全与隐私生命周期管理

DSP-07: 设计和默认数据保护
DSP-08: 设计和默认数据隐私
DSP-17: 敏感数据保护

CRC 治理、风险管理和合规

GRC-02: 风险管理计划
GRC-05: 信息安全计划

HRS 人力资源

HRS-09: 人员角色和职责
HRS-11: 信息安全意识培训

IAM 身份与访问管理

IAM-03: 身份清单
IAM-08: 用户访问评审

IVS 基础设施与虚拟化安全

IVS-02: 变更检测
IVS-03: 网络层安全
IVS-04: 操作系统加固与基线控制

LOG 日志记录和监控

LOG-03: 安全监控与告警
LOG-05: 审计日志监控与响应
LOG-12: 访问控制日志

SEF 安全事件管理，电子发现及云举证

SEF-03 事件响应计划
SEF-04 事件响应测试
SEF-06 事态鉴别分类流程

TVM 威胁和漏洞管理

TVM-07 漏洞识别
TVM-08 漏洞优先级
TVM-09 漏洞管理报告

	Stride威胁分析	引用链接
✓	身份欺骗	1. Major Security Misconfiguration Impacting ServiceNow Instances Discovered https://appomni.com/press_release/2022-major-security-misconfiguration-impacting-servicenow-and-other-saas-instances-discovered/Major Security Misconfiguration Impacting ServiceNow and Other SaaS Instances Discoveredhttps://appomni.com/resources/aolabs/appomni-discovers-security-misconfiguration-impacting-servicenow/ServiceNow Shared Security Model and Access Control Information https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB1095978ServiceNow releases guidance on Access Control List misconfigurations https://www.zdnet.com/article/servicenow-releases-guidance-on-access-control-list-misconfigurations-after-report-highlights-prevalence/ 2. UnderstandingHowFacebookDisappearedfromtheInternet https://blog.cloudflare.com/october-2021-facebook-outage/Update about the October 4th outage https://engineering.fb.com/2021/10/04/networking-traffic/outage/ More details about the October 4 outage https://engineering.fb.com/2021/10/05/networking-traffic/outage-details/Why Facebook, Instagram, andWhatsApp AllWent DownToday https://www.wired.com/story/why-facebook-instagram-whatsapp-went-down-outage/ 3. Report:SoftwareCompaniesExposedtoHackinginMajorData Breachhttps://www.vpnmentor.com/blog/report-microsoft-dynamics-leak/ *附加链接：* 4. Report:HotelReservationPlatformLeavesMillionsofPeople Exposed in Massive Data Breach https://www.websiteplanet.com/blog/prestige-soft-breach-report/ Leaky AWS S3 bucket once again at centre of data breach https://www.computerweekly.com/news/252491842/Leaky-AWS-S3-bucket-once-again-at-centre-of-data-breach 5. Unsecured-aws-server-exposed-airport-employee-records-3tb-in-datahttps://www.zdnet.com/article/unsecured-aws-server-exposed-airport-employee-records-3tb-in-data/ 6. https://www.zdnet.com/article/amazon-steps-in-to-close-exposed-flexbooker-bucket-after-december-data-breach/
✓	篡改数据	
✓	抵赖	
✓	信息泄露	
✓	拒绝服务	
✓	权限提升	

威胁 4:
缺乏云安全架构和战略

云安全战略和安全架构包括对云部署模型、云服务模型、云服务供应商（CSP）、服务区域可用域、特定云服务、一般原则[1]，和预先决定[2]的考虑和选择。此外，IAM[3]的前瞻性设计，以及跨不同云帐户、供应商、服务和环境的网络和安全控制也在范围内。战略的考虑应该先于设计并决定设计，但云挑战通常需要增量式和敏捷的规划方法。

安全责任

- ✓ 客户
- ✗ 云服务供应商
- ✗ 共同

架构

- ✓ 应用程序
- ✓ 元数据
- ✓ 信息
- ✓ 基础设施

云服务模型

- ✓ 软件即服务 (SaaS)
- ✓ 平台即服务(PaaS)
- ✓ 基础设施即服务(IaaS)

变革的快节奏和普遍化的、去中心化的、自助化的云基础设施管理方法阻碍了人们的技术和业务因素考量以及有意识的设计。然而，云要实现成功和安全，就不能忽视安全考虑和风险。行业违规案例表明，缺乏此类规划可能导致云环境和应用程序无法抵御网络攻击，或无法有效抵御网络攻击。应对好这些挑战有助于更轻松地实施云安全战略和设计。

业务影响

缺乏云安全战略和架构限制了高效企业和基础设施安全架构实施的可行性。其实现离不开这些安全/合规目标。否则，将导致罚款和违规，或者由于实施变通办法、重构和迁移而提高成本。

关键信息

以下是一些关键信息：

[1] 一般云计算原则包括基于影响（国家或社会）考虑（“本地优先”等）的云服务供应商偏好，或者，对避免按需服务消费和计费模型的接受程度；一些人喜欢这种消费和计费模型，因为它消除了摩擦，另一些人避免，因为它使预算更不可预测。这种消费和计费模型很有趣，因为它不是二进制的，而且影响了技术设计，并且具有足够的影响力，可以将其纳入“战略”考量，在早期就予以关注。

[2] 预先决定可以包括现有的供应商锁定、在需要本地数据驻留的特定地区进行扩张的业务意图、公司范围内对特定CSP或模型的偏好（例如，我看到甚至在银行业也尝试采用的零服务器足迹）。

[3] 身份和访问管理，作为一个域，而不是一个特定的云服务。

- 公司应在云服务和基础设施设计和决策中考虑业务目标、风险、安全威胁和法律合规性。
- 进行开发时考虑到快速的变化速度和有限的集中控制，考虑更为重要的云服务和基础设施战略和设计原则并予以遵守。
- 将尽职调查和第三方供应商安全评估视为基本做法。以威胁建模、安全设计和集成作为补充，同时考虑供应商故障的影响。

案例

最近的一些案例包括：

- (2021年1月) 沃尔玛旗下的美国服装店Bonobos遭遇了大规模数据泄露，泄露了数百万消费者的个人信息。一个名为ShinyHunters的威胁组织发布了Bonobos的完整数据库（70 GB的SQL数据库，包含700万条用户记录），包括消费者的地址、电话号码、部分信用卡号码和网站订单。这是由于托管备份文件的外部云备份服务受损。可以选择访问控制、加密、供应商安全、冗余和其他领域限制影响或降低类似违规现象的可能性。[1] [2]
- (2021年7月2日) 软件开发商Kaseya收到来自客户的报告，建议在Kaseya管理的端点上执行异常行为和恶意软件。攻击者可以利用虚拟存储设备（VSA）产品中的零日漏洞绕过身份验证并运行任意命令执行。这使得攻击者能够利用标准VSA产品功能将勒索软件部署到管理服务供应商（MSP）客户端（即客户端的客户端）的端点。由于对部署在不同环境中的软件进行自动零接触更新的策略，以及特定的关键软件变更管理SaaS模型，这一故障影响了许多客户；供应商和消费者可以重新考虑此策略，以限制未来的类似攻击。[3]

CSA云计算关键领域安全指南 v4.0

领域 1: 云计算概念和架构

领域 2: 治理与企业风险管理

领域 6: 管理平面和业务连续性

CSA云控制矩阵 v4.0

A&A 审计与保障

A&A-03 基于风险的规划评估
A&A-04 需求合规

AIS 应用程序和接口安全

AIS-04 应用程序安全设计和安全开发

BCR 业务连续性管理和运营韧性

BCR-02 风险评估和影响分析
BCR-03 业务连续性策略
BCR-04 业务连续性规划
BCR-08 备份

CEK 密码学、加密与密钥管理

CEK-08 云服务客户密钥管理能力
CEK-07 加密风险管理

DCS 数据中心安全

CS-01 场外设备处置的策略和规程

DSP 数据安全与隐私生命周期管理

GRC-02: 风险管理计划
GRC-05: 信息安全计划

GRC 治理、风险管理和合规

GRC-08 特殊利益团体
GRC-02 风险管理计划

IAM 身份与访问管理

IAM-04 职责分离
IAM-05 最小权限
IAM-09 特权访问角色的隔离
IAM-01 身份与访问管理的策略与规程
IAM-06 用户访问授权

IPY 互操作性与可移植性

IPY-01 互操作性与可移植性的策略与规程

IVS 基础设施与虚拟化安全

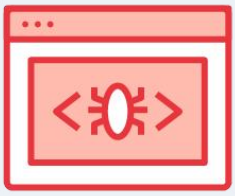
IVS-03 网络层安全
IVS-05 生产与非生产环境
IVS-08 网络架构文档
IVS-06 分区与隔离

STA 供应链管理，透明度和问责制

STA-01 共享安全责任模型的策略与规程
STA-08 供应链风险管理

	Stride威胁分析	引用链接
✓	身份欺骗	1. Incident Overview & Technical Details https://helpdesk.kaseya.com/hc/en-gb/articles/4403584098961 2. IndependenceDay:REvilusessupplychainexploittoattack hundreds of businesseshttps://news.sophos.com/en-us/2021/07/04/independence-day-revil-uses-supply-chain-exploit-to-attack-hundreds-of-businesses/ 3. DatabreachatBonoboshitsupto7million:Whattodo [updated]https://www.tomsguide.com/news/bonobos-data-breach-7-million
✓	篡改数据	
✓	抵赖	
✓	信息泄露	
✓	拒绝服务	
✓	权限提升	

威胁 5:
不安全的软件开发



软件是复杂的，云技术往往会进一步增加复杂性。这种复杂的情况下可能会出现意外的功能，导致漏洞利用[1]和可能的错误配置。由于云的可访问性，威胁者比以往任何时候都更容易利用这些“特性”。

采用“云优先”的战略态势，可以让实体将维护和安全问题转移给云服务供应商（CSP）。委托CSP管理基础设施和/或平台层避免了开发人员浪费时间做无用功。提供密钥存储/管理和安全持续集成/持续部署（CI/CD）的服务允许开发人员将重点放在业务逻辑上。

安全责任
✓ 客户
✓ 云服务供应商
✓ 共同
架构
✓ 应用程序　✗ 元数据
✗ 信息　✗ 基础设施
云服务模型
✓ 软件即服务 (SaaS)
✓ 平台即服务(PaaS)
✓ 基础设施即服务(IaaS)

CSP将提供身份和访问管理（IAM）特性，为开发者提供审查工具和正确实施指导。让公司无需自己构建服务，从而释放了资源，可投资于更具影响力的业务优先项目。

确保每个开发者都理解到公司与服务供应商共同承担一些责任。例如，如果报告了Kubernetes的零日漏洞攻击，并且一家公司正在利用CSP的Kubernetes解决方案，则CSP有责任解决该问题。使用云原生技术的Web应用程序出现的业务错误应当由开发人员负责修复。在任何一种情况下，因漏洞而产生的信息泄露都会影响公司。

没有开发人员希望创建不安全的软件。然而，主要软件供应商每月都会发布补丁，修复可能影响系统机密性、完整性和/或可用性的漏洞。并非所有的软件漏洞都有安全隐患，但历史已经证明，即使是极小的漏洞也可能最终成为重大威胁[2]。拥抱云技术可以让公司专注于其业务特有的领域，同时也应当让云服务提供商拥有和管理可能商品化的其他云服务供应事项。

业务影响

不安全的软件开发的部分业务影响包括：

- 客户对产品或解决方案失去信心
- 由于数据泄露，品牌声誉受损
- 法律诉讼导致法律和财务影响

关键信息

以下是一些关键信息：

- 使用云技术可以避免重新发明现有解决方案，从而允许开发人员能够专注于业务特有的问题。
- 通过利用责任共享模型，补丁之类的项目可以由CSP而非企业负责。
- CSPs非常重视安全，并将提供如何以安全方式实现服务的指导，例如良好的架构框架或安全的设计模式。

案例

最近的一些案例包括：

- (2021年12月9日) Log4Shell漏洞由于log4j库中的解析错误而允许RCE[3]。
- (2021年1月5日) 众所皆知的Microsoft Exchange，曾经发布的一系列漏洞，如（ProxyOracle、ProxyShell），为远程代码执行和凭据盗窃提供了多种途径[4]。
- (2021年9月13日) 苹果的iOS发现被NSO的Pegasus软件利用，利用了一个允许远程代码执行的零点击漏洞[5]。

CSA云计算关键领域安全指南 v4.0

领域 1: 云计算概念和架构

领域 10: 应用安全

领域 12: 身份、授权和访问管理

领域 13: 安全即服务

CSA云控制矩阵 v4.0

AIS 应用程序和接口安全

AIS-02：应用程序安全基线需求
AIS-04：应用程序安全设计和安全开发
AIS-05：自动化应用程序安全测试

CCC 变更控制和配置管理

CCC-02：质量测试

TVM 威胁和漏洞管理

TVM-04：检测更新

IAM 身份与访问管理

IAM-01：身份与访问管理的策略与规程
IAM-04：职责分离
IAM-05：最小权限
IAM-14：强鉴别

	Stride威胁分析	引用链接
✓	身份欺骗	1. I always call them glue bugs, I think I got that from you! https://twitter.com/taviso/status/1379447309864345602 2. AnExplorationofJSONInteroperabilityVulnerabilities https://bishopfox.com/blog/json-interoperability-vulnerabilities 3. Log4Shell:RCE0-dayexploitfoundinlog4j2,apopularJava logging packagehttps://www.lunasec.io/docs/blog/log4j-zero-day/ 4. ANewAttackSurfaceonMSExchangePart1-ProxyLogon! https://blog.orange.tw/2021/08/proxylogon-a-new-attack-surface-on-ms-exchange-part-1.html 5. AdeepdiveintoanNSOzero-clickiMessageexploit:Remote Code Execution
✓	篡改数据	
✓	抵赖	
✓	信息泄露	
✓	拒绝服务	
✓	权限提升	

威胁 6:

不安全的第三方资源

安全责任
✓ 客户
✓ 云服务供应商
✓ 共同
架构
✓ 应用程序　✓ 元数据
✓ 信息　✓ 基础设施
云服务模型
✓ 软件即服务 (SaaS)
✓ 平台即服务(PaaS)
✓ 基础设施即服务(IaaS)

在云计算应用越来越广的世界中，第三方资源可能有不同的含义：来自开源代码、通过SaaS产品和API风险（威胁2），到云供应商提供的托管服务。来自第三方资源的风险也被视为供应链漏洞，因为它们是所交付产品或服务的一部分。这些风险存在于消费的每一种产品和服务中。尽管如此，由于近年来对第三方服务和基于软件的产品越来越依赖，对这些漏洞和可破解配置的攻击也越来越多。事实上，根据科罗拉多州立大学的研究，三分之二的违规行为是供应商或第三方漏洞造成的。

因为有的产品或服务可能集合了他们使用的所有其他产品和服务，所以漏洞可以从供应链中的任何一点开始，并从那里扩散。对于恶意黑客来说，这意味着，为了实现目标，他们“只”需要寻找最薄弱的环节作为切入点。在软件领域，使用SaaS和开源进行扩展是一种常见做法。恶意黑客也有机会用同样的漏洞攻击更多的目标。

业务影响

- 关键业务流程的损失或停止。
- 业务数据被外界访问（威胁11）。
- 打补丁或修复安全问题取决于提供商及其响应速度。一旦他们提供了修复，数据的集成可能需要更新内部应用程序和产品。对业务的影响可能很大，这取决于受攻击组件对应用程序的重要性。

关键信息

以下是一些关键信息：

- 无法防止代码或产品中的漏洞，但可以尝试并正确决定使用哪种产品。使用官方支持的产品；聘用拥有合规认证证书、公开谈论安全工作、参与漏洞赏金活动、报告安全问题并快速提供修复为用户负责的人。
- 了解并跟进所使用的第三方资源。包括开源、SaaS产品、云供应商和托管服务，以及可能已经添加到应用程序中的其他集成。您也不想在受害者名单公布时，才知道自己一直在使用易受攻击的产品。
- 定期审查第三方资源。如果发现不需要的产品，请将其删除，并撤销可能授予这些产品对代码库、基础设置或应用程序的任何访问或权限。
- 不要成为最薄弱的环节。在适合公司规模的范围内渗透测试应用程序，让开发人员重视安全编码，并使用静态应用程序安全测试（SAST）和动态应用程序安全测试（DAST）解决方案。

案例

最近的一些案例包括：

- (2020年12月13日到2021年4月6日) Solarwinds是一家总部位于美国的网络监控公司。2020年，据报道，数千名政府和私企客户在一次使用不同载体的供应链攻击中受到伤害，从Solarwinds网络和产品进入其客户的网络、接触凭证和私人数据。这次攻击的真正影响仍然未知。由于敏感数据渗漏，一些组织不得不重建其整个网络和服务器。 [1] [2]

- (2021年12月) Log4shell是广受欢迎的开源Java日志框架Log4j中发现的一个零日漏洞。该漏洞于2021年11月被披露并于几天后修复。由于该框架的普及，它被认为是有史以来最大的漏洞。攻击者将此漏洞用于加密挖掘、勒索软件攻击、僵尸网络和垃圾邮件。[3] [4]

- (2019 年5月到2021年8月) 从2019年5月到2021 8月，大众汽车的北美子公司遭受了一家供应商造成的数据泄露，该供应商将存储服务置于无保护状态近两年。被破坏的数据包括个人识别信息（PII）以及一些客户更敏感的财务数据，涉及330万客户。[5] [6]

CSA云计算关键领域安全指南 v4.0

领域 1: 云计算概念和架构

领域 2: 治理与企业风险管理

领域 7: 基础设施安全

领域 10: 应用安全

领域 12: 身份、授权和访问管理

CSA云控制矩阵 v4.0

BCR 业务连续性管理和运营韧性

BCR-01: 业务连续性管理策略和规程
BCR-02: 风险评估和影响分析
BCR-03: 业务连续性策略

CCC 变更控制和配置管理

CCC-02: 质量测试
CCC-04: 未经授权的变更保护

DCS 数据中心安全

DCS-05: 资产分级分类
DCS-06: 资产登记与跟踪
DCS-07: 受控接入点

DSP 数据安全与隐私生命周期管理

DSP-03: 数据清单
DSP-05: 数据流文档
DSP-06: 数据所有权和管理权
DSP-08: 设计和默认数据隐私
DSP-10: 敏感数据传输

IAM 身份与访问管理

IAM-05: 最小权限
IAM-10: 特权访问角色的管理
IAM-11: 云服务客户对特权访问角色的批准
IAM-14: 强鉴别

IPY 互操作性与可移植性

IPY-01: 互操作性与可移植性的策略与规程
IPY-02: 应用程序接口可用性
IPY-03: 互操作性与可移植性管理的安全保护
IPY-04: 数据可移植性的合同义务

SEF 安全事件管理，电子发现及云举证

SEF-01: 安全事件管理的策略与规程
SEF-03: 事件响应计划

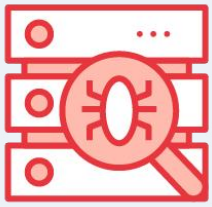
STA 供应链管理，透明度和问责制

STA-01: 共享安全责任模型的策略与规程
STA-02: 共享安全责任模型供应链
STA-03: 共享安全责任模型指南
STA-04: 共享安全责任模型控制所有权
STA-05: 共享安全责任模型文档评审
STA-06: 共享安全责任模型控制实施STA-07: 供应链清单
STA-08: 供应链风险管理
STA-09: 基本服务及合同协议
STA-10: 供应链协议评审
STA-11: 内部合规评测
STA-12: 供应链服务协议合规
STA-13: 供应链治理评审
STA-14: 供应链数据安全评估

	Stride威胁分析	引用链接
✗	身份欺骗	1. Solarwinds the supply chain hack https://www.zdnet.com/article/microsoft-fireeye-confirm-solarwinds-supply-chain-attack/ 2. Using Microsoft for the Solarwinds hack https://www.reuters.com/article/us-global-cyber-usa-idUSKBN28Y1BF 3. Log4Jhackhttps://blog.cloudflare.com/inside-the-log4j2-vulnerability-cve-2021-44228/ 4. More than 1.2m attacks using log4j https://www.ft.com/content/d3c244f2-eaba-4c46-9a51-b28fc13d9551 5. Volkswagen and Audi customer's data leakage https://www.bleepingcomputer.com/news/security/audi-volkswagen-data-breach-affects-33-million-customers/ 6. Two third of breaches are supply chain attacks https://www.nationaldefensemagazine.org/articles/2020/7/2/hackers-putting-global-supply-chain-at-risk
✗	篡改数据	
✓	抵赖	
✓	信息泄露	
✗	拒绝服务	
✓	权限提升	

威胁 7：

系统漏洞



安全责任
✓ 客户
✓ 云服务供应商
✓ 共同
架构
✓ 应用程序　✓ 元数据
✓ 信息　✓ 基础设施
云服务模型
✓ 软件即服务 (SaaS)
✓ 平台即服务(PaaS)
✓ 基础设施即服务(IaaS)

系统漏洞是目前云服务平台中普遍存在的缺陷。攻击者可能会利用它们破坏数据的机密性、完整性和可用性，从而破坏服务运营。值得注意的是，所有组件都可能包含使云服务易受攻击的漏洞。实施针对以下漏洞的安全强化措施对于降低安全风险至关重要。

主要有以下4类系统漏洞：

- 零日（zero-day）漏洞-——新发现的还未开发出补丁的漏洞。黑客会迅速利用这些漏洞，因为在部署补丁之前没有任何东西可以阻止它们。之前发现的Log4Shell就是一个典型的严重的零日漏洞，影响了使用广泛部署的基于Java的Log4j日志设施的服务。
- 缺少安全补丁——一旦有已知关键漏洞的补丁，应当尽快部署，从而减少系统的攻击面。随着时间的推移，会发现新的系统漏洞，需要提供新的补丁。随着未修补漏洞数量的增加，整体系统安全风险也在增加。
- 基于配置的漏洞-——当使用默认或错误配置的设置部署系统时，就会出现这种漏洞。基于配置的漏洞示例包括使用遗留安全协议、弱加密密码、弱权限和保护不足的系统管理接口。在系统上运行不必要的服务是另一个与配置相关的问题。
- 弱凭据或默认凭据——缺乏强身份验证凭据使潜在的攻击者可以轻松访问系统资源和相关数据。同样地，未安全存储的密码可能会被黑客窃取并用于侵入系统。

业务影响

- 许多成功的数据泄露源于利用系统漏洞的攻击。IBM的《2021数据泄露成本报告》[2] 指出，第三方软件中的漏洞导致了研究对象中14%的数据泄露，而云配置错误和凭据泄露分别占20%和15%。
- 当数据泄露发生时，公司的业务可能会中断，从而阻止客户使用公司的服务。

数据泄露后，如果公司的品牌和服务不再值得信任，那么获得新客户可能会更加困难。这些后果都可能导致收入损失。

- IBM的报告确定了四个数据泄露成本中心及其每次事件的平均成本（以百万美元计）。检测和升级占29%（124万美元），通知占6%（27万美元），事后分析响应占27%（114万美元），业务损失占38%（159万美元）。每次事件的总成本为424万美元。这些案件中的数据泄露涉及2k到101k条泄露记录。对于5000万至6500万条记录的重大数据泄露，每次事件的总平均成本为4.01亿美元。

关键信息

以下是一些关键信息：

- 系统漏洞是系统组件中的缺陷，通常是由人为错误引入，使黑客更容易攻击公司的云服务。
- 事后响应的成本很高。丢失公司数据可能会对企业的收入和声誉底线产生负面影响。
- 通过常规漏洞检测和补丁部署以及严格的IAM实践，可以极大地降低系统漏洞带来的安全风险。

案例

最近的一些案例包括：

- (2021年12月9日) Log4Shell（CVE-2021-45046）远程代码漏洞，影响了基于Java的日志记录工具Log4j 2.0beta9至2.14.1版本系统的使用。鉴于Java在云系统中的广泛使用，Log4Shell是一个严重威胁。攻击者可以通过向易受攻击的系统提交恶意请求来利用Log4Shell，该请求会导致系统执行任意代码，使攻击者能够窃取信息、启动勒索软件或接管系统的控制权。CISA、FBI、NSA和其他政府组织预计Log4Shell在很长时间都会被利用。[1]
- (2021年8月) 云安全公司Wiz的安全研究人员透露，他们可以访问数千名Microsoft Azure客户的数据。Azure的CosmosDB中存在安全漏洞，研究人员将其命名为ChaosDB，该漏洞允许用户在没有用户凭据的情况下下载、删除或以其他方式操作数据。[2]

- (2021年9月) 微软的研究人员观察到一个与俄罗斯政府有联系的网络间谍组织部署了一个后门，利用ActiveDirectory Federation窃取配置数据库和安全令牌。微软将该恶意软件称为FoggyWeb，并将其归因于俄罗斯黑客组织APT29（又名Cozy Bear和NOBELIUM）。[2]
- (2021年) 根据软件厂商Ivanti的《2021勒索软件聚焦年终报告》，与勒索软件攻击相关的漏洞数量从2020年的233个增加到2021的288个，增长了29%。[3]

CSA云计算关键领域安全指南 v4.0

领域 7: 基础设施安全

领域 10: 应用安全

领域 11: 数据安全和加密

领域 12: 身份、授权和访问管理

CSA云控制矩阵 v4.0

AIS 应用程序和接口安全

AIS-01: 应用程序和接口安全策略和规程
AIS-02: 应用程序安全基线需求
AIS-06: 自动化应用程序安全部署

CEK 密码学、加密与密钥管理

CEK-03: 数据加密
CEK-04: 加密算法

IAM 身份与访问管理

IAM-02: 强密码的策略与规程
IAM-14: 强鉴别
IAM-15: 密码管理
IAM-16: 授权机制

IVS 基础设施与虚拟化安全

IVS-04: 操作系统加固与基线控制

TVM 威胁和漏洞管理

TVM-01: 威胁与漏洞管理的策略及规程
TVM-02: 恶意软件防护的策略和规程
TVM-03: 漏洞修复措施安排
TVM-04: 检测更新
TVM-05: 外部库漏洞
TVM-06: 渗透测试
TVM-07: 漏洞识别
TVM-08: 漏洞优先级
TVM-09: 漏洞管理报告

	Stride威胁分析	引用链接
✓	身份欺骗	1. Log4Shell 0-day Vulnerability: All You Need to Know https://jfrog.com/blog/log4shell-0-day-vulnerability-all-you-need-to-know/ 2. Microsoft's very bad year for security: A timeline https://www.csoonline.com/article/3635849/microsofts-very-bad-year-for-security-a-timeline.html 3. Ransomware SpotlightYear End 2021 Report (Ivanti) https://www.ivanti.de/lp/security/reports/ransomware-spotlight-year-end-2021-report 附加链接： 1. 2021 marks another record year for security vulnerabilities https://www.techrepublic.com/article/2021-marks-another-record-year-for-security-vulnerabilities/ 2. Cost of Data Breach Report (IBM) https://www.ibm.com/security/data-breach 3. Cybersecurity vulnerabilities and their business impact https://www.verizon.com/business/resources/articles/s/cyber-security-vulnerabilities-and-their-business-impact 4. MitigatingLog#ShellandOtherLog4j-RelatedVulnerabilities https://www.cisa.gov/uscert/ncas/alerts/aa21-356a 5. TheInternetisonFirehttps://www.wired.com/story/log4j-flaw-hacking-internet/ 6. Ransomware attacks are increasingly exploiting security vulnerabilties https://www.techrepublic.com/article/ransomware-attacks-are-increasingly-exploiting-security-vulnerabilities/ 7. Top Routinely Exploited Vulnerabilities https://www.cisa.gov/uscert/ncas/alerts/aa21-209a 8. What are the different types of vulnerabilities? https://www.packetlabs.net/types-of-vulnerabilities/
✓	篡改数据	
✗	抵赖	
✓	信息泄露	
✗	拒绝服务	
✓	权限提升	

威胁 8:
云计算数据的意外泄露

安全责任
✓ 客户
✓ 云服务供应商
✓ 共同
架构
✓ 应用程序　✓ 元数据
✓ 信息　✗ 基础设施
云服务模型
✓ 软件即服务 (SaaS)
✓ 平台即服务(PaaS)
✓ 基础设施即服务(IaaS)

云服务使公司能够以前所未有的速度建设、创新和扩展。然而，云和向云服务所有权的转变的复杂性，以及团队和业务单位的多样性，往往导致缺乏安全治理和控制。不同CSP云资源配置数量的增加使错误配置更加普遍，云库存缺乏透明度和网络可视性可能会导致数据意外泄露。

数据暴露仍然很普遍。超过55%的公司至少有一个数据库目前公开暴露在互联网上[1]。许多数据库使用弱密码或不需要身份验证，使其成为攻击者不断扫描互联网搜索此类暴露数据库的易攻击目标。不安全的Elasticsearch服务器可能在八小时内被破坏[2]。必须尽快修复此类风险。

业务影响

云的易用性，特别是可以灵活设置托管数据库和存储对象的速度，使其非常受欢迎。这些数据中可能包含敏感的客户数据、员工信息、产品数据等。暴露此类数据会导致意外费用，如取证团队、客户支持流程产生的费用以及受影响客户的赔偿。

根据IBM的研究报告[3]，2021年，数据泄露成本从386万美元增至424万美元。报告中，IBM提到了数据泄露还会产生很多额外的间接成本，例如内部调查和沟通、当前客户流失以及由于信誉受损而导致的潜在客户流失等。

关键信息

为了避免无意的数据泄露，建议云客户可以做到以下几点：

1. 查看PaaS数据库、存储和计算工作负载托管数据库，包括虚拟机、容器以及安装在其上的数据库软件。因为基于配置的解决方案提供必要可见性的能力有限，无法检查或扫描工作负载。

2. 选择完全可见整个企业云环境的暴露引擎，识别允许流量暴露在外部的任何路由或网络服务，包括负载均衡器、应用程序负载均衡器、内容分发网络（CDN）、网络对等互连、云防火墙、Kubernetes网络等。
3. 确保数据库实施最低权限的IAM策略，并通过控制和监控该策略的分配减少访问风险。

案例

最近的一些案例包括：

- 2021年1月, VIP Games 23M 数据——云错误配置暴露了超过6万用户的2300万条记录，包括电子邮件、用户名、社交问题、网络ID和网页玩家数据[4]。
- 2021 年4月, Reverb 5.6M数据——Elasticsearch存储的560万条客户记录在网上公开[5]。
- 2021年9月, The Telegraph 10TB 数据——英国报纸《电讯报》披露了一个包含用户数据的10TB的数据[6]。
- 2022年1月, Securita, 1M 数据——未经验证的AWS服务器暴露了3TB的机场员工数据[7]。
- 2022 年2月, FlexBooker 19M 数据——12月数据泄露后，亚马逊关闭了FlexBooker bucket。[8]

CSA云计算关键领域安全指南 v4.0

领域 5: 信息治理

领域 7: 基础设施安全

领域 12: 身份、授权和访问管理

CSA云控制矩阵 v4.0

AIS 应用程序和接口安全

AIS-02：应用程序安全基线需求
AIS-04：应用程序安全设计和安全开发

IAM 身份与访问管理

IAM-01：身份与访问管理的策略与规程
IAM-03：身份清单

BCR 业务连续性管理和运营韧性

BCR-05：文档记录

DSP 数据安全与隐私生命周期管理

DSP-03：数据清单
DSP-08：设计和默认数据保护

GRC 治理、风险管理和合规

GRC-01：治理计划的策略和规程
GRC-02：风险管理计划

IVS 基础设施与虚拟化安全

IVS-01：基础设施与虚拟化的安全策略与规程
IVS-03：网络层安全
IVS-06：分区与隔离

Stride威胁分析		引用链接
✗	身份欺骗	1.2022 Cloud Security Threats report https://www.wiz.io/ty/2022-cloud-security-threats-report 2.Unsecured Elasticsearch server breached in eight hours flat https://www.computerweekly.com/news/252484365/Unsecured-ElasticSearch-server-breached-in-eight-hours-flat 3.How much does a data breach cost? https://www.ibm.com/security/data-breach 4.A cloud misconfiguration exposed 23M records of over 60K users containingemails,usernames,socialnetworkID,andplayerdataon thewehttps://portswigger.net/daily-swig/online-gaming-platform-vip-games-exposes-23-million-data-records-on-misconfigured-server 5.Elasticsearchstoring5.6Mcustomerrecordswasexposedontheweb https://www.bitdefender.com/blog/hotforsecurity/etsy-owned-musical-instrument-marketplace-reverb-suffers-data-breach 6.UK newspaper The Telegraph exposed 10TB database with subscriberdata https://securityaffairs.co/wordpress/123020/data-breach/the-telegraph-data-leak.html 7.UnauthenticatedAWSserverexposed3TBinairportemployeerecords https://www.zdnet.com/article/unsecured-aws-server-exposed-airport-employee-records-3tb-in-data/ 8.AmazonstepsintocloseexposedFlexBookerbucketafterDecember databreach https://www.zdnet.com/article/amazon-steps-in-to-close-exposed-flexbooker-bucket-after-december-data-breach/
✓	篡改数据	
✓	抵赖	
✓	信息泄露	
✗	拒绝服务	
✗	权限提升	

威胁 9：

无服务器和容器化工作负载的配置不当和利用

迁移到云基础设施和采用DevOps实践使IT团队能够比以往更快地为业务提供价值。管理和扩展基础设施和安全控制以运行应用程序仍然是开发团队的重大挑战。用于管理内部部署（on-prem）环境的遗留基础设施团队必须学习新技能，如基础设施代码和云安全。这些团队必须对支持其应用程序的网络和安全控制承担更多责任。无服务器和云原生容器化工作负载似乎是解决这个问题的灵丹妙药—将责任转移给云服务提供商。不过，与将虚拟机迁移到云相比，它需要更高级别的云和应用程序安全成熟度。

安全责任	
✓ 客户	
✓ 云服务供应商	
✓ 共同	
架构	
✗ 应用程序	✓ 元数据
✓ 信息	✗ 基础设施
云服务模型	
✗ 软件即服务 (SaaS)	
✓ 平台即服务(PaaS)	
✓ 基础设施即服务(IaaS)	

在无服务器模型中，CSP负责底层基础架构的安全和管理。除了开发和运营方面的优势之外，还减少了攻击面，因为默认情况下CSP在短期容器中运行功能代码。不断刷新的系统显著限制了攻击事件的持久性。但是，如果CSP允许客户配置具有更长生命周期和“热启动”配置的无服务器容器，那么环境的安全性就会降低。其他风险包括临时文件系统和共享内存，也可能泄漏敏感信息。临时存储器的访问可能用于托管或执行恶意软件，应用程序代码应清除这些访问。

无服务器责任模型产生了一个更加微妙和复杂的环境。在云网络安全公司Netskope进行的分析中，所分析的IAM策略中有4%具有完全管理权限，60%具有AWS Administrator Access角色[1]。如果将这些权限分配给一个面向公众的AWS无服务器Lambda函数，则漏洞可能会很多。允许访问云环境、敏感数据泄漏或AWS账户接管都可能发生。

对基础设施缺乏控制也限制了缓解应用程序安全问题的措施和传统安全工具的可见性。这使得为了减少攻击的辐射半径，围绕云健康、应用程序安全、可观察性、访问控制和密钥管理建立强大的组织变得至关重要。

业务影响

无服务器和容器化工作负载可以显著提高云计算应用的敏捷性、降低成本、简化操作，甚至提高安全性。但在缺乏必要专业知识和尽职调查的情况下，使用这些技术实施的应用程序配置可能会导致重大违规、数据丢失甚至资金枯竭。

关键信息

以下是一些关键信息：

- 企业应通过云安全态势管理（CSPM）、云基础设施授权管理（CIEM）和云工作负载保护平台（CWPP）实施自动检查。
- 企业应投资云安全培训、治理流程和可重用的安全云架构模式，以降低不安全云配置的风险和频率。
- 开发团队在迁移至移除传统安全控制的无服务器技术之前，应更加严格地遵循安全和工程相关的最佳实践。

案例

最近的一些案例包括：

- 截至2021，关于拒绝钱包（DoW）攻击的研究越来越多。DoW攻击在功能上类似于拒绝服务（DoS）攻击。DoS攻击者向无服务器应用程序发送大量请求，以影响底层基础结构。但在DoW攻击中，目标是利用无服务器平台的弹性伸缩消费模型，让云客户支付大额费用。这些攻击可以通过并发限制缓解，但这会将攻击向量从DoW转为DoS。[2]
- (2021年) 在不同的容器运行时和环境中发现了多个逃逸漏洞，包括CVE-2022-0811（CRI-O容器逃逸漏洞）[3] 、CVE-2022-0185（Linux内核缓冲区溢出）[4]和Azurescape漏洞[5]。这些漏洞中的每一个都有可能使攻击者逃离容器环境并获得对容器主机的特权访问。Azurescape漏洞发生时，甚至允许在另一个Azure客户的Azure容器实例环境中运行代码。
- (2022年2月) Cado实验室的研究人员发现了直接针对第一个AWS Lambda的已知恶意软件的证据，他们将该软件命名为Denonia。一些人积极使用Denonia。

> Denonia是一个用来挖掘Monero加密货币的Lambda函数，通过使用DNS over HTTPS与C2服务器通信。虽然该恶意软件不会利用Lambda中的任何漏洞进行攻击，并且需要管理权限才能部署，但它是攻击者使用无服务器环境获取经济利益的一个示例，损害了企业的利益。[6]

CSA云计算关键领域安全指南 v4.0

领域 1: 云计算概念和架构

领域 2: 治理与企业风险管理

领域 4: 合规和审计管理

领域 5: 信息治理

领域 6: 管理平面和业务连续性

领域 7: 基础设施安全

领域 8: 虚拟化和容器

领域 9: 事件响应

领域 10: 应用安全

领域 11: 数据安全和加密

领域 12: 身份、授权和访问管理

CSA云控制矩阵 v4.0

A&A 审计与保障

A&A-02: 独立评估
A&A-03: 基于风险的规划评估
A&A-04: 需求合规
A&A-05: 审计管理流程
A&A-06: 修复措施

CEK 密码学、加密与密钥管理

CEK-03: 数据加密
CEK-05: 加密变更管理

AIS 应用程序和接口安全

AIS-02：应用程序安全基线需求
AIS-03：应用程序安全指标
AIS-04：应用程序安全设计和安全开发
AIS-05：自动化应用程序安全测试
AIS-06：自动化应用程序安全部署

BCR 业务连续性管理和运营韧性

BCR-02：风险评估和影响分析
BCR-03：业务连续性策略

CCC 变更控制和配置管理

CCC-02：质量测试
CCC-04：未经授权的变更保护
CCC-09：变更恢复

LOG 日志记录和监控

LOG-03：安全监控与告警
LOG-05：审计日志监控与响应
LOG-12：访问控制日志

SEF 安全事件管理，电子发现及云举证

SEF-03 事件响应计划
SEF-04 事件响应测试
SEF-06 事态鉴别分类流程

DSP 数据安全与隐私生命周期管理

DSP-07：设计和默认数据保护
DSP-08：设计和默认数据隐私
DSP-17：敏感数据保护

IAM 身份与访问管理

IAM-03：身份清单
IAM-05：最小权限
IAM-09：特权访问角色的隔离
IAM-10：特权访问角色的管理
IAM-14：强鉴别

IVS 基础设施与虚拟化安全

IVS-02：容量与资源规划
IVS-03：网络层安全
IVS-04：操作系统加固与基线控制
IVS-05：生产与非生产环境
IVS-07：迁移到云环境

TVM 威胁与漏洞管理

TVM-07 漏洞识别
TVM-08 漏洞优先级
TVM-09 漏洞管理报告

	Stride威胁分析	引用链接
✗	身份欺骗	1. A-real-world-look-at-aws-best-practices-iam-policies https://www.netskope.com/blog/a-real-world-look-at-aws-best-practices-iam-policies 2. S221421262100079Xhttps://www.sciencedirect.com/science/article/pii/S221421262100079X 3. Cri-o-vulnerabilityhttps://blog.aquasec.com/cve-2022-0811-cri-o-vulnerability 4. Linux-kernel-container-escape-in-kubernetes https://blog.aquasec.com/cve-2022-0185-linux-kernel-container-escape-in-kubernetes 5. Azure Escape https://www.paloaltonetworks.com/blog/2021/09/azurescape/ 6. First-malware-targeting-aws-lambdahttps://thehackernews.com/2022/04/first-malware-targeting-aws-lambda.html
✓	篡改数据	
✓	抵赖	
✓	信息泄露	
✓	拒绝服务	
✓	权限提升	

威胁 10：

有组织的犯罪、黑客和APT攻击

安全责任
✓ 客户
✓ 云服务供应商
✓ 共同
架构
✓ 应用程序　✓ 元数据
✓ 信息　✓ 基础设施
云服务模型
✓ 软件即服务 (SaaS)
✓ 平台即服务(PaaS)
✓ 基础设施即服务(IaaS)

高级持续性威胁（APT）是一个范围很广的术语，是一种入侵者或入侵者团队在网络上进行长期非法攻击以挖掘高度敏感数据的攻击活动。[1]这些小组可能包括国家和有组织犯罪团伙。“有组织犯罪”一词是用来描述在实施体现组织个体努力、有计划、有逻辑的行为时，组织所具有的组织水平的方式 [5]。APT领域已经建立了复杂的战术、技术和方案（TTP）实现攻击目标。数月仍未在目标网络中发现APT组织并不罕见这段时间又允许他们横向移动到高度敏感的业务数据或资产。一些APT组织历来青睐特定行业或组织，如能源和航空部门。APT组织可能因各种动机实施恶意活动，如政治或经济活动。

威胁情报机构密切研究APT组织。威胁情报报告鼓励不同组织和国家多了解APT组织及其行为。可以通过模拟报告中描述的APT组织的行为，开展红队演练更好地保护自己。此类网络演习允许开展与APT组织相关的各种TTP测试和提高其网络检测能力。还应开展威胁搜寻活动，检测其网络中是否存在APT。

业务影响

- APT组织的动机各不相同。有些是出于政治动机（即黑客活动主义者），而另一些则是有组织的犯罪集团的一部分，甚至还有一些团体是国家支持的威胁组织。
- 要了解APT组织对一个组织的业务影响，必须对其信息资产进行业务影响分析，从而能够理解APT组织如何和为什么可能以某个组织为目标，以及潜在安全漏洞可能对业务产生的潜在影响。

关键信息

以下是一些关键信息：

- 对所在的组织进行业务影响分析，了解信息资产。
- 参与网络安全信息共享小组，以了解任何相关的APT组织及其TTP。
- 进行攻击性安全演习，以模拟这些APT组织的TTP，并调整安全监控工具以检测。

案例

最近的案例包括：

- (2022年1月21日) LAPSUS$组织侵入了英伟达的内部网络并窃取了机密数据。该组织没有向英伟达勒索数据，而是要求释放对用于加密挖掘的图形处理单元的限制。[4]

CSA云计算关键领域安全指南 v4.0

领域 9: 事件响应

领域 13: 安全即服务

CSA云控制矩阵 v4.0

TVM 应用程序和接口安全

TVM-01: 威胁与漏洞管理的策略及规程
TVM-02: 恶意软件防护的策略和规程
TVM-03: 漏洞修复措施安排
TVM-04: 检测更新
TVM-05: 外部库漏洞
TVM-06: 渗透测试
TVM-07: 漏洞识别
TVM-08: 漏洞优先级
TVM-09: 漏洞管理报告
TVM-10: 漏洞管理指标

LOG 日志记录和监控

LOG-03 安全监控与告警
LOG-05 审计日志监控与响应

	Stride威胁分析	引用链接
✓	身份欺骗	1.APTDefinitionhttps://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/ 2.Chinese APT Group Targeting Global MSPs: https://www.securityweek.com/symantec-chinese-apt-group-targeting-global-msps 3.HowNorthKoreaalmostpulledoffabillion-dollarhack: https://www.bbc.com/news/stories-57520169 4.Lapsus$ group demanding Nvidia release restrictions on crypto mining on itsGPUs:https://cybersecuritynews.com/beware-lapsus-ransomware-group/ 5.Cyber Organized Crime: What is it? https://www.unodc.org/e4j/en/cybercrime/module-13/key-issues/cyber-organized-crime_what-is-it.html
✓	篡改数据	
✓	抵赖	
✓	信息泄露	
✓	拒绝服务	
✓	权限提升	

威胁 11：

云存储数据泄露

安全责任
✓ 客户
✓ 云服务供应商
✓ 共同
架构
✓ 应用程序　✓ 元数据
✓ 信息　✗ 基础设施
云服务模型
✓ 软件即服务 (SaaS)
✓ 平台即服务(PaaS)
✓ 基础设施即服务(IaaS)

云存储数据泄露是一种涉及敏感、受保护或机密信息的事件。这些数据可能会被组织之外的个人发布、查看、窃取或使用。数据泄露可能是有针对性攻击的主要目标，并且可能是由漏洞利用、配置错误、应用程序漏洞或不良的安全实践造成的。泄露的数据可能涉及任何不打算公开发布的信息，例如个人健康信息、财务信息、个人身份信息（PII）、商业秘密和知识产权等。

数据泄露场景中，受害者通常不会意识到数据丢失。如果攻击者想让受害者知道，如直接获得财务收益或勒索软件，可能会通知受害者。尽管如此，有些情况下，人们不知道数据泄露的事实，或者在很长一段时间后才发现，这使得任何缓解措施都显得不太重要。

由于数据是一项主要资产，云的易用性、配置、弹性、韧性以及适合所有合理需求的多种服务使云数据存储极具吸引力。也因为这些，很多情况都可能发生泄露。可能由于人为错误或滥用导致数据泄露，例如PaaS服务的错误配置。存储对象还可能暴露通过个人云存储应用程序在外部共享的敏感数据或文件。

云存储数据泄露还可能始于网络钓鱼攻击，即操纵应用程序或服务。最初发生泄露的载体可能导致凭据被盗或未经授权访问云数据。攻击者继而可能采取一些潜在的行动，如提取数据以供进一步使用，同时加密组织的数据以发起勒索软件攻击。

供应链攻击可能提供对底层数据的访问，使检测和恢复更加复杂。随着组织向零信任模式迈进，传统的组织边界发挥的作用越来越小。最小特权访问和基于身份的安全控制应限制数据暴露。实施云态势管理也很重要，以符合CSP的最佳实践或监管基线以及攻击检测和数据灾难恢复机制。

业务影响

数据泄露有几个潜在的影响：

- 知识产权丢失，智力成果可能被他人用于产品开发、战略规划，甚至发动未来攻击。
- 失去客户、利益相关者、合作伙伴和员工的信任，可能会抑制商业行为、投资和购买，并降低员工在该组织工作的意愿。
- 监管更严格，包括财务罚款或流程和业务变更等。
- 地缘政治因素会影响商业行为。
- 员工对组织保护员工数据的能力失去信任。

关键信息

以下是一些关键信息：

- 云存储需要一个配置良好的环境（SSPM、CSPM）。
- 应用CSP最佳实践指南、监控和检测功能，以检测和防止攻击及数据泄露。
- 需要对员工进行云存储使用安全意识培训，因为数据分散在不同的位置并由不同的角色控制。
- 在适当的情况下实施客户端加密。
- 对数据进行分类从而采取不同的控制措施，记录事件响应中所采取的措施。

案例

最近的一些案例包括：

- (2021年6月24日) “因2019年发生重大用户数据泄露事件，Facebook在欧洲受到起诉，但该事件直到在黑客论坛上发现其有超过5.33亿个账户信息可供免费下载后才被曝光。”[1]
- (2019年3月11日) “安全研究人员发现，数十家公司无意中泄露了敏感的公司和客户数据，因为员工将公司Box存储账号中的文件链接公之于众，很容易识别到信息。”[2]
- (2022年4月12日) “亚马逊周一宣布，最近解决了亚马逊关系型数据库服务（RDS）中可能导致内部凭据泄露的漏洞。”[3]

领域 2: 治理与企业风险管理

领域 3: 法律问题，合同和电子举证

领域 4: 合规和审计管理

领域 5: 信息治理

领域 6: 管理平面和业务连续性

领域 7: 基础设施安全

领域 9: 事件响应

领域 10: 应用安全

领域 11: 数据安全和加密

领域 12: 身份、授权和访问管理

领域 13: 安全即服务

CSA云控制矩阵 v4.0

A&A 审计与保障

A&A-02: 独立评估
A&A-04: 需求合规

AIS 应用程序和接口安全

AIS-01: 应用程序和接口安全策略和规程
AIS-04: 应用程序安全设计和安全开发
AIS-07: 应用程序漏洞修复措施

CCC 变更控制和配置管理

CCC-03: 变更管理技术
CCC-04: 未经授权的变更保护
CCC-07: 基线偏离检测

DSP 数据安全与隐私生命周期管理

DSP-03: 数据清单
DSP-04: 数据分级分类
DSP-07: 设计和默认数据保护
DSP-08: 设计和默认数据隐私
DSP-10: 敏感数据传输
DSP-17: 敏感数据保护

GRC 治理、风险管理和合规

GRC-01: 治理计划的策略和规程
GRC-08: 特殊利益团体

HRS 人力资源

HRS-04: 远程与居家工作的策略与规程
HRS-11: 信息安全意识培训

CEK 密码学、加密与密钥管理

CEK-03：数据加密
CEK-19：密钥泄露

DCS 数据中心安全

DCS-02：场外传输授权的策略和规程

IVS 基础设施与虚拟化安全

IVS-04：操作系统加固与基线控制
IVS-09：网络防御

IPY 互操作性与可移植性

IPY-03：互操作性与可移植性管理的安全保护

LOG 日志记录和监控

LOG-03：安全监控与告警
LOG-05：审计日志监控与响应
LOG-12：访问控制日志

SEF 安全事件管理，电子发现及云举证

SEF-03：事件响应计划
SEF-06：事态鉴别分类流程

IAM 身份与访问管理

IAM-03：身份清单
IAM-07：用户访问变更与撤销
IAM-14：强鉴别
IAM-16：授权机制

STA 供应链管理，透明度和问责制

STA-02：共享安全责任模型供应链
STA-06：共享安全责任模型控制实施
STA-07：供应链清单
STA-08：供应链风险管理
STA-14：供应链数据安全评估

TVM 威胁和漏洞管理

TVM-02：恶意软件防护的策略和规程
TVM-04：检测更新
TVM-07：漏洞识别

UEM 统一终端管理

UEM-09：反恶意软件检测与防范
UEM-14：第三方终端安全态势

	Stride威胁分析	引用链接
✓	身份欺骗	1. Facebookfaces‘massaction’lawsuitinEuropeover2019 breachhttps://techcrunch.com/2021/04/16/facebook-faces-mass-action-lawsuit-in-europe-over-2019-breach/ 2. Dozens of companies leaked sensitive data thanks to misconfigured Box accountshttps://techcrunch.com/2019/03/11/data-leak-box-accounts/ 3. Amazon RDS Vulnerability Led to Exposure of Credentials https://www.securityweek.com/amazon-rds-vulnerability-led-exposure-credentials
✓	篡改数据	
✓	抵赖	
✓	信息泄露	
✓	拒绝服务	
✓	权限提升	

结论

随着云业务模型和安全策略的发展，本报告提高了人们对云计算关键威胁的认识，例如（1）身份、凭据、访问和密钥管理不足；（2）不安全的接口和API；（3）配置不当和变更控制不足；（4）缺乏云安全架构和战略。其他突出威胁有（5）不安全的软件开发、（6）不安全的第三方资源、（7）系统漏洞。

身份、凭据、访问和密钥管理不足成为首要威胁。重播攻击、冒名顶替和过度许可在云环境中和在内部部署的一样持续存在，很容易进行访问。使用自签名证书、不良的密码管理或信任每个根CA证书只是几种存在问题的做法。随着对零信任架构和SDP的强调，难怪本报告中强调的此类案例是调查对象最关心的。

微服务的持续采用显示了安全接口和API的重要性。应该会有更多这样的功能，值得关注的是，在保护这些功能方面仍然面临重大挑战，而云在这些功能的开发中所起的作用微乎其微。随着这些API扩散到SaaS和PaaS产品中，编码人员的低效率和云的始终在线特性带来了重大风险。

配置错误和变更控制不足在2019年的顶级威胁报告中排名第二。这是云问题在安全架构中越来越受到重视的另一个例子。几十年来，配置管理一直是组织能力成熟度的一部分，在团队接受云之前，都会面临该问题。云的持久网络访问和无限容量的错误配置可能会影响公司内的许多机构。

最后，在2019年的列表中排名第三的战略和架构引出了一个问题："为什么在规划和架构安全解决方案方面仍然存在这样的问题？"云计算已不再是一种新奇事物——需要定义一种全局方法并执行相应的架构设计模式。

这份《云计算的11类顶级威胁》报告延续了2019年度顶级威胁报告的趋势，但关注点从传统的信息安全（如漏洞和恶意软件）转移到新的方向。无论如何，这些威胁是发展和增强云安全意识、配置和身份管理的行动要求。云本身不会造成困扰，所以现在更关注云技术的实现。