云计算的 11 类顶级威胁

cloud security alliance

感谢我们的赞助商

云安全联盟（CSA）是一个非营利性的、由成员推动的组织，致力于定义最佳实践及提高对它的认识，以确保安全的云计算环境。基于行业从业者、协会、政府、以及企业和个人会员的专业知识，CSA 提供云安全研究、教育、认证、活动和产品。CSA 的活动、知识和广泛的网络使受云计算影响的整个社区—从提供商和客户，到政府、企业家和保证行业—都受益匪浅，并提供了一个论坛，让不同的各方可以通过这个论坛共同创造和维护一个值得信赖的云生态系统。CSA 研究以独立于厂商的中立、灵活和结果的完整为荣。

感谢 ExtraHop 为研究的发展提供资金支持，并确保 CSA 研究生命周期内的质量控制。

ExtraHop 是 CSA 企业会员，他们支持研究项目的研究成果，但对 CSA 研究的内容开发或编辑权没有额外的影响。

目录

鸣谢

主席

Jon-Michael C. Brook

贡献者

Jon-Michael C. Brook
Alexander Getsin
Greg Jensen
Laurie Jameson
Michael Roza
Neha Thethi
Ashish Kurmi
Shachaf Levy
Shira Shamban
Vic Hargrave
Victor Chin
Zoran Lalic
Randall Brooks

云安全联盟全球成员

Victor Chin
Stephen Lumpe (Cover Art)
AnnMarie Ulskey (Design)

修订记录

日期	批准	注解
2019 年 8 月 6 日	John Yeoh	原文刊载
2019 年 10 月 1 日	John Yeoh	勘误，略作调整
2020 年 2 月 4 日	John Yeoh	增加赞助商
2020 年 4 月 8 日	Frank Guanco	少量更新

中文版翻译说明

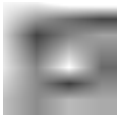
由云安全联盟大中华区（CSA GCR）秘书处组织翻译《云计算的 11 类顶级威胁》(Top Threats to Cloud Computing The Egregious 11)，云安全联盟大中华区专家翻译并审校。

翻译审校工作专家：（按字母顺序排序）

组长：沈勇

组员：陈皓、伏伟任、高巍、江楠（腾讯云）、靳明星（易安联）、李岩、刘宇馨（奇安信）、欧建军、唐宇（龙湖集团）、王安宇（OPPO）、王贵宗、王永霞（腾讯云）、杨喜龙、于乐、余晓光（华为）、张威

在此感谢以上参与该文档的翻译审校工作的专家及工作人员。如译文有不妥当之处，敬请读者联系 CSA GCR 秘书处给与雅正！联系邮箱：info@c-csa.cn；云安全联盟 CSA 公众号：



序言

如今，越来越多的企业正在将数据和应用程序迁移到云中，这带来了独特的信息安全挑战。而企业在使用云计算服务时将面临 11 个主要的云安全威胁。保护企业在云中数据的主要责任并完全不在于服务提供商，而主要在于客户本身。为了使组织对云安全问题有新的了解，以便他们可以就云采用策略做出有根据的决策，云安全联盟 CSA 发布了新版本的《云计算的 11 类顶级威胁》，报告反映了 CSA 安全专家之间当前就云中重要的安全问题达成的共识。尽管云中存在许多安全问题，但这个列表主要关注 11 个与云计算的共享、按需特性相关的问题。本报告由 CSA 全球云威胁工作组专家们原创，大中华区云安全专家们翻译，相信与以前的各版本那样对近期开始云转型和已经采用云服务的企业会有所帮助。

李雨航 Yale Li

CSA 大中华区主席兼研究院院长

概要

“顶级威胁”报告一贯旨在提高对云平台威胁，风险和漏洞的认识。此类问题通常由云计算按需和共享的天生特征导致。在第四部分中，我们再次就云行业安全问题与241位行业专家进行调查。今年，我们的受访者对其云环境中的11个主要威胁，风险和漏洞进行了评估。最高威胁工作组结合调查结果及专业知识来撰写2019年最终报告（“本报告”）。

最新报告按调查结果重要程度着重介绍了前11个威胁（括号中是以往的排名）：

1.数据泄露（1）
2.配置错误和变更控制不足
3.缺乏云安全架构和策略
4.身份，凭证，访问和密钥管理不足
5.帐户劫持（5）
6.内部威胁（6）
7.不安全的接口和API（3）
8.控制平面薄弱
9.元结构和应用程序结构失效
10.有限的云使用可见性
11.滥用及违法使用云服务（10）

观察和理由

在分析了此调查的所有回复之后，我们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有所下降。拒绝服务，共享技术漏洞以及云服务提供商数据丢失和系统漏洞之类的担忧（在以前的潜在风险 TOP 12中都具有）现在的评分非常低，已不在本报告之列。这表明，由云服务提供商负责的传统安全问题似乎已经有效的缓解。相反，我们看到更多的是需要解决那些位于技术栈更高层次的安全问题，这些问题是高级管理层决策的结果。

在调查中，评分最高的新项目更加细微，表明消费者对云的理解日益成熟。这些问

题本质上是云计算的固有特性，表明消费者正在积极考虑向云迁移的技术环境。这些主题涉及潜在的控制平面缺陷，元结构和应用结构故障以及有限的云可见性。这些新的重点与以前的《 关键威胁（Top Threats）》报告中更为突出的通用威胁，风险和漏洞（即数据丢失，拒绝服务）明显不同。

我们希望本报告能够提高组织对最重要的安全问题及其应对措施的认识，并确保在为云迁移和安全性制定预算时将其考虑在内。该报告提供了控制建议和参考示例，旨在供合规，风险和技术人员使用。管理层也能够从本报告的技术趋势和概述中受益。

1. 安全问题：数据泄露

数据泄露是指敏感、受保护或机密信息被未经授权的个人发布、查看、窃取或使用的网络安全事件。数据泄露可能是蓄意攻击的主要目的，也可能仅仅是人为错误、应用程序漏洞或安全措施不足的结果。数据泄露涉及任何非公开发布的信息，包括但不限于个人健康信息、财务信息、个人可识别信息（PII）、商业秘密和知识产权。

历史排名
顶级威胁 1 ⟷ 顶级威胁 1
安全责任
☒客户 ☒云服务供应商 ☑两者皆有
架构
☑应用程序 ☑信息 ☑元数据 ☑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

数据泄露的负面后果可能包括：

1.对客户或合作伙伴声誉和信任的影响
2.丢失应对竞争对手的知识产权，可能影响产品发布
3.监管影响：可能导致的财务损失
4.品牌影响：由于上述原因导致的市场价值减少
5.法律和合同责任
6.应急响应和取证所产生的财务花销

有一些数据泄露的情况在发生后几个月才被发现。在此类事件中，其影响可能不会

立即显现（例如，知识产权盗窃）。例如，美国人事管理办公室（OPM）和索尼电影公司的数据泄露都有大约一年的迟滞时间。

关键信息

1.数据正成为网络攻击的主要目标。对于拥有或处理数据的组织而言，定义数据的业务价值及其丢失的影响非常重要。

2.保护数据正在演变成一个谁有权访问数据的问题。

3.通过互联网访问的数据是最容易被错误配置或利用的漏洞资产。

4.加密技术可以帮助保护数据，但会对系统性能产生负面影响，同时降低应用程序的用户友好性。

5.一个稳健且经过充分测试的应急响应计划，考虑到云服务供应商(CSP)和数据隐私法，将有助于数据泄露受害者恢复。

案例

- 由于云计算环境的破坏，Timehop 的数据泄露影响了 2100 万用户。社交媒体访问令牌也遭到破坏。
- Uber 披露，其亚马逊网络服务（AWS）账户在 2016 年底遭到黑客攻击，全球 5700 万用户的个人信息受到损害。
- 2019 年，提供互联网语音协议（VoIP）服务的电信公司 Voipo 公布了数以百万计的客户通话日志、短消息服务（SMS）日志和凭证。该数据库于 2018 年 6 月公开，其中包含可追溯至 2015 年 5 月的通话和消息日志。许多文件都包含详细的通话记录（即谁给谁打电话、通话时间等）。Voipo 总共暴露了“700 万个通话记录、600 万条短信和包含未加密密码的内部文档，如果使用这些密码，攻击者可以深入访问该公司的系统。

CSA 安全指南

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 9: 事件响应

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

CCM 控制项

AIS 应用程序和接口安全
AIS-01: 应用程序安全
AIS-02: 客户访问要求
AIS-03: 数据完整性
AIS-04: 数据安全/完整性

CCC 变更控制和配置管理
CCC-05: 生产变更

DSI 数据安全与信息生命周期管理
DSI-01:分类
DSI-02: 数据目录/数据流
DSI-03: 电子商务交易
DSI-04: 处理/标示/安全策略
DSI-05: 非生产数据
DSI-07: 安全处置

EKM 加密与密钥管理
EKM-01: 权限
EKM-02: 密钥生成
EKM-03: 敏感数据保护
EKM-04:存储与访问

GRM 治理与风险管理
GRM-02: 关注数据的风险评估
GRM-06: 策略
GRM-10: 风险评估

IAM 身份与访问控制
IAM-01: 审计工具访问
IAM-04: 策略和规程

威胁分析	链接和引用
☒身份欺骗 ☒篡改数据 ☒抵赖 ☑信息泄露 ☒拒绝服务 ☒权限提升	1. Timehop Security Incident, July 4, 2018: https://www.timehop.com/ security/ 2. Uber Discloses Year-Old AWS Data Breach, Exposing Millions of Users: https://awsinsider.net/articles/2017/11/21/uber-aws-data-breach.aspx 3. Amazon hit with major data breach days before Black Friday: https://www.theguardian.com/technology/2018/nov/21/amazon-hit-with-major-databreach-days-before-black-friday 4. VOIPO database exposed millions of call and SMS logs, system data: https://www.zdnet.com/article/voipo-database-exposed-millions-of-calland-sms-logs-system-data/

2. 安全问题：配置错误和变更控制不足

当计算资产设置不正确时，就会产生配置错误，这时常会使它们面对恶意活动时倍显脆弱。一些常见的例子包括：

- 不安全的数据存储要素（元素）或容器
- 过多的权限
- 默认凭证和配置设置保持不变
- 标准的安全控制措施被禁用

历史排名
新的顶级威胁
安全责任
☑客户 ☒云服务供应商 ☒客户和云服务提供商
架构
☑应用架构 ☑信息架构 ☑元数据架构 ☑基础设施架构
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）

云资源的配置错误是导致数据泄露的主要原因，可能会导致删除或修改资源以及服务中断。

在云环境中，缺乏有效的变更控制是导致配置错误的常见原因。云环境和云计算方法与传统信息技术(IT)的不同之处在于，它们使变更更难控制。 传统的变更流程涉及多个角色和批准，可能需要几天或几周才能到达生产阶段（环境）。

企业数据中心中静态的基础设施元素现在被抽象为云中的软件，它们的整个生命周期可能只持续几分钟或几秒钟。云计算技术依赖于自动化、角色扩展和访问来支持快速变更。使用多个云提供商会增加复杂性，因为每个提供商都有独特的能力，这些能力几乎每天都会得到增强和扩展。这种动态环境需要一种敏捷和主动的方法来进行变更控制和补救，但许多公司还没有精通这种方法。

业务影响

配置项错误的业务影响可能非常严重，这取决于配置错误的性质以及发现和缓解的速度。最常见被报告的影响是云存储库中的数据暴露。

关键信息

1. 基于云的资源高度复杂并具有动态性，因此配置具有挑战性。
2. 传统的控制和变更管理方法在云计算中是无效的。
3. 公司应该拥抱自动化，并引入持续扫描配置错误的资源和实时修复问题的技术。

案例

最近的配置错误和变更控制不足问题的例子包括:

1. 2017 年，一个配置错误的 AWS 简单（对象）存储服务 S3（Simple Storage Service)云存储桶（bucket）泄露了 1.23 亿美国家庭的详细私人数据。数据集属于信用机构益博睿(Experian)，该公司将数据出售给一家名为 Alteryx 的在线营销和数据分析公司。是 Alteryx 泄露了文件。
2. 2018 年，Exactis 的一个不安全的 Elasticsearch 数据库再次遭到大规模泄露，其中包含 2.3 亿美国消费者的详细个人数据。原因是数据库服务器被配置为可公开访问。
3. 2018 年，专门从事自动化过程和装配的工程公司 Level One Robotics（Level One），泄露了大众、克莱斯勒、福特、丰田、通用汽车、特斯拉和蒂森克虏伯等 100 多家制造企业高敏感度的专有信息。在本例中，配置错误的资产是一个 rsync(备份)服务器，它允许将未经身份验证的数据传输到任何 rsync 客户端。

CSA 安全指南

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

CCM 控制项

AIS 应用程序和接口安全
AIS-01: 应用程序安全
AIS-04: 数据安全/完整性

EKM 加密与密钥管理
EKM-03: 敏感数据保护
EKM-04: 存储与访问

CCC 变更控制和配置管理
CCC-02: 外包开发
CCC-03: 质量测试
CCC-05: 生产变更

GRM 治理与风险管理
GRM-01: 基线要求
GRM-02: 关注数据的风险评估

DSI 数据安全与信息生命周期管理
DSI-01:分类
DSI-04: 处理/标示/安全策略

HRS 人力资源安全
HRS-09: 培训/意识

IVS 基础设施与虚拟化安全
IVS-02: 变更检测
IVS-06: 网络安全
IVS-07: 操作系统加固和基础控制措
IVS-06: 网络安全
IVS-07: 操作系统加固和基础控制措

IAM 身份与访问控制
IAM-02:凭证生命周期/提供管理
IAM-05: 职责分离

威胁分析	链接和引用
☒身份欺骗 ☑篡改数据 ☑抵赖 ☑信息泄露 ☑拒绝服务 ☒权限提升	*1.120 Million American Households Exposed in 'Massive' ConsumerView Database Leak :* https://www.forbes.com/sites/thomasbrewster/2017/12/19/120m-american-households-exposed-inmassive-consumerview-database-leak/#37bb94d27961 *2. Marketing Firm Exactis Leaked a Personal Info Database with 340 Million Records:* https://www.wired.com/story/exactis-database-leak-340-millionrecords/ 3. *Short Circuit: How a Robotics Vendor Exposed Confidential Data for Major Manufacturing Companies:* https://www.upguard.com/breaches/short-circuit-how-a-robotics-vendor-exposed-confidential-data-for-majormanufacturing-companies

3. 安全问题：缺乏云安全架构和策略

放眼全球，各组织均在逐步把他们的部分 IT 基础设施迁移到公有云之上。在迁移过渡期中，最大的挑战之一就是实现能够承受网络攻击的安全架构。不幸的是，这个过程对于很多组织而言仍然是模糊不清的。当组织把上云迁移判定为简单的将现有的 IT 栈和安全控制“直接迁移（搬家式）”到云环境的过程，这时候数据就被暴露在各种威胁面前。缺乏对于共享安全责任模型的理解也是另外一个诱因。

历史排名
新的顶级威胁
安全责任
☑客户 ☒云服务提供商 ☒两者皆有
架构
☒应用架构 ☒信息架构 ☒元数据 ☑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（PaaS）

另外，通常而言迁移过程中功能性和速度通常是优先于安全考虑的。这些因素导致了下云迁移过程中云安全架构和策略缺失的组织容易成为网络攻击的受害者。实现适合的安全体系结构和开发健壮的安全策略将为组织在云上开展业务活动提供坚实的基础。利用云原生工具来增加云环境中的可视化，也可以最小化风险和成本。如果采取这些预防措施，可以显著降低安全风险。

业务影响

无论公司规模大小，对于云上迁移、部署、使用而言，合适的安全架构和策略都是必要的。成功的网络攻击会对业务造成严重的影响，包括财务损失、声誉受损、法律后果和罚款等。

关键信息

1. 确保安全架构与业务目标和预期一致。
2. 开发和实现安全架构框架
3. 确保威胁模型的持续更新
4. 对于整体安全态势提供持续监控

案例

有关云安全架构和策略缺失问题的相关案例如下

- 2017 年，云计算技术巨头埃森哲(Accenture)最近证实，该公司无意中在四个不安全的 Amazon S3 存储桶中留存了大量私人数据，如果暴露了高度敏感的口令和解密密钥，这可能会对公司和客户造成相当大的损害。S3 存储桶包括了几百 GB 的云商企业数据，亚马逊也表示该产品同时为大多数财富 100 强公司提供产品支持。这些数据可以在无需密码情况下被任何知道该服务器地址的人员直接下载。
- 安全中心的研究员表示发现了本田 Connect App 上的大量数据在网上曝光。这些数据存储在两个不安全的、可被公开访问的、不受保护的 Amazon AWS S3 存储桶中。

CSA 安全指南

领域 1: 云计算概念和体系架构

领域 6: 管理平面和业务连续性

领域 7: 基础设施安全

CCM 控制项

AIS 应用程序与接口安全
AIS-04: 数据安全/完整性

GRM 治理与风险管理
GRM-01: 基线要求
GRM-02: 关注数据的风险评估
GRM-05: 管理层支持/参与
GRM-08: 风险评估对策略的影响

IAM 身份与访问控制
IAM-02: 凭证生命周期/提供管理

IVS 基础设施与虚拟化安全
IVS-06: 网络安全
IVS-08: 生产/非生产环境
IVS-09: 隔离
IVS-13: 网络架构

STA 供应链管理，透明与可审计
STA-03: 网络/基础设施
STA-05: 供应链协议

威胁分析	链接和引用
☑身份欺骗 ☑篡改数据 ☑抵赖 ☑信息泄露 ☑拒绝服务 ☑权限提升	1. Introduction to Cloud Security Architecture from a Cloud Consumer's Perspective: https://www.infoq.com/articles/cloud-security-architecture-intro 2. The New Shared Responsibility Model For Cloud Security: https://www.forbes.com/sites/forbestechcouncil/2018/10/15/the-new-sharedresponsibility-model-for-cloud-security/#508d0f422490 3. The Importance of a Defined Cloud Strategy: https://www.expedient.com/blog/the-importance-of-a-defined-cloud-strategy/ 4. Accenture left a huge trove of highly sensitive data on exposed servers: https://www.zdnet.com/article/accenture-left-a-huge-trove-of-clientpasswords-on-exposed-servers/ 5. The Consequences of a Cyber Security Breach: https://www.sungardas.com/en/about/resources/articles/the-consequences-of-a-cyber-security-breach/ 6. Why Enterprise Architecture Deserves a Seat at the Security Table: https://erwin.com/blog/enterprise-architecture-seat-security-table/ 7. Personal data of over 50,000 Honda Connect App leaked: https://www.hackread.com/personal-data-of-over-50000-honda-connect-app-leaked/

4. 安全问题：身份，凭据，访问和密钥管理的不足

资源访问的管理、监视和保护的工具和策略。例如包括电子文件、计算机系统和物理资源（如服务器机房和建筑物）。

历史排名
新的顶级威胁
安全责任
☑客户 ☒云服务提供商 ☒两者皆
架构
☒应用架构 ☒信息架构 ☒元数据 ☑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)

云计算对传统内部系统的身份和访问管理（IAM）方面引入了多种变化。这些不一定是新问题。 相反，在云计算中这些是更重要的问题，因为云计算会深刻影响身份，凭据和访问管理。在公有云和私有云设置中，都需要云服务提供商（CSPs）和云服务使用者在不损害安全性的情况下管理IAM。

由于以下原因，可能会造成安全事件及数据泄露：

- 凭据保护不足
- 缺乏加密秘钥、密码和证书的定期自动更新机制
- 缺乏可扩展的身份、凭据及访问控制系统
- 无法使用多因子认证方式
- 无法使用强密码

凭证及加密密钥不能嵌入到源代码或发布到公共代码库中（如 GitHub），因为存在泄漏和滥用的风险。需要使用安全性良好的公钥基础结构（PKI）对密钥进行适当的保护，以确保进行密钥管理活动。

身份管理系统要具有可扩展性，能够对无数用户及云服务提供者全生命周期管理。身份管理系统须支持人员变更从而立即取消对资源访问，例如工作离职或角色变化。这

些身份全生命周期管理过程需自动集成到云环境中并及时完成。

身份管理系统逐渐变成内部关联的。云服务提供者的联合身份管理（如安全断言标记语言 SAML）变得更加普遍以降低用户维护的负担。企业计划使用云服务提供商的联合身份管理机制必须理解云服务提供商的身份解决方案的相关安全性，包括过程、基础设施及不同用户间的隔离（在共享身份管理方案的情况下）。最佳实践需要针对对于特权用户及云服务运营商（例如，云客户）的多因子身份认证系统，例如智能卡、一次性密码（OTP）及电话身份认证。

这些形式的认证有助于解决密码盗用问题，即未经过用户允许的情况下对资源进行访问。密码盗用可表现为常见的网络横向移动攻击，例如“哈希传递攻击”。

在旧系统仅支持密码的情况下，认证系统必须支持策略实施，例如强密码验证及企业定义的密码周期轮换策略。

用来保护数据的加密秘钥管理必须贯彻全生命周期，包括密钥生成、分发、存储、替换及销毁。

这样做有助于解决针对未经授权访问密钥的攻击。加密秘钥失窃再加上秘钥轮换策略缺失，可能会大大增加失效时间和范围。

包含数据秘密（例如密码，私钥或机密的客户联系数据库）的任何集中式存储机制都是攻击者的高价值目标。选择集中密码及秘钥管理是组织必须仔细考虑的折衷方案：既要考虑集中秘钥管理的便利性，又要考虑秘钥被攻击的威胁。对于高价值资产，对身份及秘钥管理系统的监控和保护是重中之重。

业务影响

冒充合法用户，操作员或开发人员的恶意行为者可以：

- 读取、窃取、更新及删除数据
- 发布控制面及管理功能
- 监听传输中的数据
- 发布看似来自合法来源的恶意软件

综上，身份、凭证或密钥管理不足会导致对数据的未经授权的访问，并可能对组织或最终用户造成灾难性的破坏。

关键信息

1. 安全帐户，包括两因素身份验证，并限制根帐户的使用。
2. 对云用户和云账号采用严格的身份和访问控制
3. 根据业务需求和最小特权原则进行隔离、细分帐户及对虚拟私有云（VPC）和身份分组
4. 定期更新密钥，删除未使用的凭据或访问权限，并采用集中式编程密钥管理。

案例

与身份，凭证，访问和密钥管理不足有关的问题的最新示例包括：

- 在 2018 年 11 月，一名德国学生入侵了受弱密码保护的数据，并使用云平台共享了该信息。这位 20 岁的年轻人利用“ Iloveyou”和“ 1234”之类的密码入侵了数百名他不喜欢其政治立场的议员和人士的在线帐户。德国网络安全官员透露，与 1,000 名国会议员，记者和其他公众人物相关的电话号码，短信，照片，信用卡号码和其他数据已通过 Twitter 和其他在线平台被盗，整理和散布。
- 会计公司 Deloitte 于 2017 年 9 月 25 日由于身份，凭据和访问管理薄弱而遭受重大数据泄露，当时该公司宣布由于管理员电子邮件帐户安全性差而检测到其全球电子邮件服务器受到破坏。此次妥协发生在 2017 年 3 月，据称使攻击者享有“到所有区域”的特权，不受限制的访问权限。管理员帐户仅需要一个密码，而无需采用两步验证过程。 据称，攻击者自 2016 年 10 月/ 11 月以来一直控制着服务器。Deloitte 的 244,000 名员工利用 Microsoft Azure 云服务存储传入和传出的电子邮件。除电子邮件外，黑客可能还可以访问用户名，密码，Internet 协议（IP）地址，企业架构图和健康信息。 有些电子邮件带有带有敏感安全性和设计详细信息的附件。此外，黑客可能已经访问了该组织蓝筹客户的用户名，密码和个人数据。
- 2017 年 5 月 31 日，威胁参与者使用 OneLogin 的 AWS 密钥从中间主机与美国另一家较小的服务提供商通过应用程序编程接口（API）获得对公司 AWS 平台的访问。提供身份和密码管理服务的 OneLogin 检测到入侵并关闭受影响的系统（和受到破坏的 AWS 密钥）以在几分钟之内停止入侵。 他们还确认没有其他活动威胁。
- 攻击者最近从 GitHub 上获取了云服务凭据，并劫持了一个账户来开采虚拟货币。GitHub 项目中包含的云服务提供商凭据在项目上线后 36 小时内被发现并被滥用。
- 总部位于德克萨斯州奥斯汀的信息安全解决方案提供商 Praetorian 推出了一个新的基于云的平台，该平台利用 Amazon AWS 的计算能力来破解密码哈希。

CSA 安全指南

领域 11：数据安全和加密

领域 12：身份、授权和访问管理

CCM 控制项

EKM 加密与密钥管理

EKM-01: 权限
EKM-02: 密钥生成
EKM-03: 敏感数据保护
EKM-04: 存储与访问

HRS 人力资源安全

HRS-01: 资产归还
HRS-03: 任用协议
HRS-04: 任用终止
HRS-08: 技术可接受使用
HRS-09: 培训/意识
HRS-10: 用户职责

IAM 身份与访问控制

IAM-01: 审计工具访问
IAM-02: 凭证生命周期/提供管理
IAM-03: 诊断/配置端口访问
IAM-04: 策略和规程
IAM-05: 职责分离
IAM-06: 源代码访问限制
IAM-07: 第三方访问
IAM-08: 可信源
IAM-09: 用户访问授权
IAM-10: 用户访问评审
IAM-11: 用户访问撤销
IAM-12: 用户 ID 身份凭证

威胁分析	链接和引用
☑身份欺骗 ☑篡改数据 ☑抵赖 ☑信息泄露 ☑拒绝服务 ☑权限提升	1. *German Man Confesses to Hacking Politicians' Data, Officials Say:* https://www.nytimes.com/2019/01/08/world/europe/germany-hacking-arrest.html 2. *German data hacker says he was 'annoyed' by politicians:* https://www.irishtimes.com/news/world/europe/german-data-hacker-says-he-wasannoyed-by-politicians-1.3751332 3. *Deloitte hit by cyber-attack revealing clients' secret emails:* https://www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyber-attackrevealing-clients-secret-emails 4. *Deloitte breached by hackers for months:* https://blog.malwarebytes.com/security-world/2017/09/deloitte-breached-by-hackers-for-months/ 5. *Major identity manager breach exposes sensitive user info:* https://www.engadget.com/2017/06/03/major-identity-manager-breach-stole sensitive-user-info/?guccounter=1 6. *OneLogin, May 31, 2017 Security Incident:* https://www.onelogin.com/blog/may-31-2017-security-incident 7. *System Shock: How A Cloud Leak Exposed Accenture's Business:* https://www.upguard.com/breaches/cloud-leak-accenture 8. *Quora breach leaks data on over 100 million users:* https://www.engadget.com/2018/12/03/quora-breach/ 9. *Attackers Scrape GitHub for Cloud Service Credentials, Hijack Account to Mine Virtual Currency:* http://www.forbes.com/sites/runasandvik/2014/01/14/attackers-scrape-github-for-cloud-servicecredentials-hijack-account-to-mine-virtual-currency/ 10. *Dell Releases Fix for Root Certificate Fail:* http://www.bankinfosecurity.com/dell-releases-fix-for-root-certificate-fail-a-8701/op-1

5. 安全问题：账户劫持

帐户劫持是一种威胁，在这种威胁中，恶意攻击者可能获得并滥用特权或敏感帐户。在云环境中，风险最高的帐户是云服务或订阅账户。网络钓鱼攻击、对基于云的系统的入侵或登录凭据被盗等都可能会危害这些帐户。这些独特、潜在且非常强大的威胁可能会导致云环境的严重中断例如数据和资产丢失和系统入侵等。这些风险源于云服务的交付模型及其组织和治理的交付模型数据和应用程序驻留在云服务中，而云服务驻留在云中帐户或订阅里。特别是订阅，任何具有特权和登录凭据的人都可以在线访问。

历史排名
顶级威胁 5 ⟷ 顶级威胁 5
安全责任
☑客户 ☑云服务提供商 ☑两者皆有
架构
☑应用架构 ☒信息架构 ☑元数据 ☒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)

组织应大力提高对这些威胁的认知意识，并采取纵深防御的保护策略来遏制破坏。

业务影响

帐户和服务劫持意味着完全的失陷：对帐户、其服务以及内部数据的控制。在这种情况下，跟帐户相关的所有业务逻辑、功能、数据和应用程序都有风险

这种失陷的后果有时很严重。在最近的泄露案例中，出现了严重的运营和业务中断，包括组织资产、数据和能力完全丧失的例子。

账户劫持的后果包括导致声誉受损的数据泄露、品牌价值下降、涉及法律责任以及敏感的个人和商业信息泄露。

关键信息

1. 帐户劫持是一个必须认真对待的威胁，处置措施不仅仅只是密码重置。
2. 纵深防御和 IAM 控制是减轻账户劫持的关键。

案例

最近与账户劫持有关的事件包括：

•2014 年 6 月，前代码托管服务公司 Code Spaces 的 AWS 账户因未能通过多因素身份验证保护其管理控制台而被入侵，这家企业在资产遭到破坏后被迫关闭。

•2017 年标志着针对云帐户的活动的兴起，特别是针对 Microsoft Office 365 的活动。

•2010 年 4 月，亚马逊跨站点脚本（XSS）漏洞导致凭证被盗，2009 年，众多亚马逊系统被劫持运行宙斯僵尸网络病毒。

CSA 安全指南

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

领域 9: 事件响应

领域 12: 身份、授权和访问管理

CCM 控制项

BCR 业务连续性管理与运营恢复

BCR-01: 业务连续性的策划

IAM 身份与访问控制

IAM-02: 凭证生命周期/提供管理

IAM-05: 职责分离

IAM-08: 可信源

IAM-10: 用户访问评审

IAM-11: 用户访问撤销

IVS 基础设施与虚拟化安全

IVS-01: 审计日志/入侵检测

IVS-08: 生产/非生产环境

SEF 安全事件管理，电子发现与云取证

SEF-01: 联络人/监管机构维护

威胁分析	链接和引用
☑身份欺骗 ☑篡改数据 ☑抵赖 ☑信息泄露 ☑拒绝服务 ☑权限提升	1. Murder in the Amazon cloud: https://www.infoworld.com/article/2608076/data-center/murder-in-the-amazon-cloud.html 2. Alleged hacker tried to sell details of 319 million iCloud users for bitcoin: https://www.cultofmac.com/583836/alleged-hacker-tried-to-sell-details of-319-million-icloud-for-bitcoin/ 3. PoC Exploit Compromises Microsoft Live Accounts via Subdomain Hijacking: https://threatpost.com/poc-exploit-compromises-microsoft-live-accountsvia-subdomain-hijacking/138719/ 4. How can Office 365 phishing threats be addressed?: https://www.helpnetsecurity.com/2018/05/18/office-365-phishing-threats/

6. 安全问题：内部威胁

卡内基梅隆计算机应急响应小组（CERT）将内部威胁定义为“对组织资产拥有访问权限的个人，恶意或无意地使用其访问权限，以可能对组织造成负面影响的方式行事的可能性。”内部人员可以是在职或离职的雇员、承包商或其他值得信赖的商业伙伴。与外部威胁参与者不同，内部人员不必穿透防火墙、虚拟专用网络（vpn）和其他外围安全防御。内部人员在公司的安全边界内工作，得到公司信任，他们可以直接访问网络、计算机系统和敏感的公司数据。

历史排名
顶级威胁 6 ⟷ 顶级威胁 6
安全责任
☑客户 ☒云服务提供商 ☒两者皆有
架构
☒应用架构 ☒信息架构 ☒元数据 ☑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)

内部威胁比你想象的更普遍。《Netwrix 2018 云安全报告》显示，58%的公司将安全漏洞归咎于内部人员。大多数安全事故都是由内部人员疏忽引起的。

据波尼蒙研究所（Ponemon Institute）2018 年“内部人员威胁成本研究”（Cost of insider Threats study）显示，员工或承包商的疏忽是 64%报告的内部人员安全事件的根本原因，而 23%与内部人员犯罪有关，13%与凭证被盗有关。列举的一些常见场景包括配置错误的云服务器、员工将公司敏感数据存储在自己不安全的个人设备和系统上、员工或其他内部人员成为导致恶意攻击公司资产的网络钓鱼电子邮件的牺牲品。

业务影响

内部威胁可能导致专有信息和知识产权的损失。与攻击相关的系统停机时间会对公司的生产效率产生负面影响。此外，数据丢失或对其他客户伤害会降低对公司服务的信心。

处理内部安全事件涉及遏制、补救、事件响应、调查、事后分析、升级、监控和监

视。这些活动可以大大增加公司的工作量和安全预算。波尼蒙研究所（Ponemon Institute）报告称，在接受采访的公司中，2017 年（每家公司）内部事件的平均成本超过 870 万美元，最高成本高达 2650 万美元。

关键信息

1.采取措施尽量减少内部人的疏忽，可以帮助减轻内部人员威胁的后果。后续描述的措施可以帮助解决用户和管理员疏忽引起的安全问题。

2.员工安全培训和教育：为您的安全团队提供培训、配置和监视计算机系统、网络、移动设备和备份设备的培训。

3.定期培训员工安全意识：向您的员工定期提供培训，以告知他们如何处理安全风险，例如网络钓鱼和保护他们在笔记本电脑和移动设备上携带的公司外部数据。需要使用强密码和频繁的密码更新。告知员工从事恶意活动的后果。

4.修复配置错误的云服务器：定期审核云中和内部的服务器，然后纠正与整个组织中设置的安全基线的任何偏差。

5.限制对关键系统的访问：确保特权账户访问安全系统和中央服务器的员工数量限制在最低限度，并且这些人员仅包括那些受过处理计算机服务器关键任务管理培训的人员。对所有服务器上任何特权级别的访问进行监控。

案例

最近与内部威胁相关的问题包括：

•特斯拉在恶意内部人员威胁问题上的惨痛教训（2018 年）——“对特斯拉首席执行官埃隆•马斯克（Elon Musk）来说，公司可能遭受恶意内部人员威胁的潜在损害成为一个严酷的现实，他对得知自己在特斯拉内部有一名破坏者表示失望。据报道，涉嫌对特斯拉进行破坏的个人是一名因没有得到晋升而不满的员工。……（埃隆）马斯克说，破坏行动包括使用虚假户名对特斯拉生产操作系统中使用的代码进行更改，以及“向未知第三方输出大量高度敏感的特斯拉数据”。

•2018 年 6 大恶劣的内部袭击之一，“可能比特斯拉事件更具破坏性，这是印度旁遮普国家银行（Punjab National Bank）18 亿美元的内部欺诈事件。这家银行的一名员工利用极其敏感的密码未经授权访问 SWIFT 银行间交易系统，在一个高度复杂的欺诈性交易链中操作资金交易，这个交易链是由一家钻石商人策划的，目的是从供应商那里购买钻石原石。”

•2018 年 IBM X-Force 威胁情报指数－“配置错误的云服务器、网络备份事件和其他配置不当的系统导致了超过 20 亿条记录的曝光，占 X-Force 在 2017 年跟踪的受损记录总数的近 70%。”

CSA 安全指南

领域 2: 治理与企业风险管理

领域 5: 信息治理

领域 11: 数据安全和加密

领域 12: 身份、授权和访问管理

CCM 控制项

DCS 数据中心安全
DCS-04: 场外授权
DCS-08: 非授权人员进入
DCS-09: 用户访问

DSI 数据安全与信息生命周期管理
DSI-04: 处理/标示/安全策略
DSI-06: 责任人/管理者

EKM 加密与密钥管理
EKM-02: 密钥生成
EKM-03: 敏感数据保护

GRM 治理与风险管理
GRM-03: 管理者监督
GRM-04: 管理程序
GRM-06: 策略
GRM-07: 策略实施
GRM-10: 风险评估

HRS 人力资源安全
HRS-02: 背景调查
HRS-03: 任用协议
HRS-07: 角色/职责

IAM 身份与访问控制
IAM-01: 审计工具访问
IAM-05: 职责分离
IAM-08: 可信源
IAM-09: 用户访问授权
IAM-10: 用户访问评审
IAM-11: 用户访问撤销

IVS 基础设施与虚拟化安全
IVS-09: 隔离

SIA 供应链管理，透明与可审计
STA-09: 第三方审核

威胁分析	链接和引用
☑身份欺骗 ☑篡改数据 ☒抵赖 ☑信息泄露 ☒拒绝服务 ☑权限提升	1. CERT Definition of an 'Insider Threat' - Updated: https://insights.sei.cmu.edu/insider-threat/2017/03/cert-definition-of-insider-threat---updated.html 2. Cloud Security Risks and Concerns in 2018: https://blog.netwrix.com/2018/01/23/cloud-security-risks-and-concerns-in-2018/ 3. IBM X-Force Threat Intelligence Index 2018: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=77014377USEN 4. Insider Threat–2018 Statistics: https://www.uscybersecurity.net/insiderthreats-2018-statistics//2018_Global_Cost_of_a_Data_Breach_Report.pdf 5. Examining the 2018 Cost of a Data Breach: https://databreachcalculator.mybluemix.net/assets/2018_Global_Cost_of_a_Data_Breach_Report.pdf 6. Tesla's Tough Lesson on Malicious Insider Threats: https://www.infosecurity-magazine.com/news/teslas-tough-lesson-on-malicious/ 7. The 6 Worst Insider Attacks of 2018 – So Far: https://www.darkreading.com/the-6-worst-insider-attacks-of-2018---so-far/d/d-id/1332183

7. 安全问题：不安全接口和 API

历史排名
顶级威胁 3--->顶级威胁 7
安全责任
☒客户 ☒云服务提供商 ☑两者皆有
架构
☑应用架构 ☒信息架构 ☑元数据 ☑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)

云计算提供商开放了一系列软件的用户界面（UI）和 API，以允许客户管理云服务并与之交互。常见云服务的安全性和可用性取决于这些 API 的安全性。

从身份验证和访问控制到加密和活动监视，这些接口必须设计成可防御无意和恶意规避安全策略的行为。设计不良的 API 可能会被滥用，甚至数据泄露。被破坏，暴露或黑客攻击的 API 已导致了一些重大的数据泄露。组织必须了解设计接口并将它们放到 Internet 上所必须的安全要求。

API 和 UI 通常是系统中最开放的部分，可能只是在组织可信边界外具有公开 IP 地址的资产。作为“前门”，他们很有可能会遭到不断的攻击。因此，需要在设计时考虑安全问题，以及适当的控制措施来保护它们免受攻击

业务影响

尽管大多数提供商都努力确保将安全很好地集成到他们的服务模型中，但是对于这些服务的使用者来说，了解这些云服务的使用，管理，编排和监视的安全相关影响是至关重要的。使用一系列安全性薄弱的接口和 API，会使组织面对各种安全问题，如机密性，完整性，可用性和相关责任的安全问题。此外，组织在监管和财务方面也可能受到非常大的影响。

关键信息

1. 保持良好的 API 安全性。良好做法包括对目录，测试，审计和异常活动保护等进行认真监督。
2. 确保 API 密钥的有效保护并避免重复使用。
3. 考虑使用标准和开放的 API 框架(如：开放式云计算界面(OCCI)和云基础架构管理界面(CIMI))

案例

最近涉及到不安全接口和 API 的案列：

- Facebook 在 2018 年 9 月 28 日宣布了一项影响超过 5000 万个账户的重大数据泄露事件。据报道，在一年前的 2017 年 7 月，一个凭证窃取漏洞被引入到 Facebook 代码中。 该公司承认，它不知道有什么信息被盗，也不知道有多少其他用户帐户因此事件而受影响。

CSA 安全指南

领域 5: 信息治理
领域 6: 管理平面和业务连续性
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

CCM 控制项

AIS 应用程序和接口安全
AIS-01: 应用程序安全
AIS-03: 数据完整性
AIS-04: 数据安全/完整性

IAM 身份与访问控制
IAM-01: 审计工具访问
IAM-07: 第三方访问
IAM-08: 可信源

IAM-09: 用户访问授权
IAM-10: 用户访问评审
IAM-11: 用户访问撤销
IAM-12: 用户 ID 身份凭证
IAM-13: 实用程序访问

威胁分析	链接和引用
☒身份欺骗 ☑篡改数据 ☑抵赖 ☑信息泄露 ☒拒绝服务 ☑权限提升	1. *Murder in the Amazon cloud:* https://www.infoworld.com/article/2608076/data-center/murder-in-the-amazon-cloud.html 2. *Alleged hacker tried to sell details of 319 million iCloud users for bitcoin:* https://www.cultofmac.com/583836/alleged-hacker-tried-to-sell-detailsof-319-million-icloud-for-bitcoin/ 3. *PoC Exploit Compromises Microsoft Live Accounts via Subdomain Hijacking:* https://threatpost.com/poc-exploit-compromises-microsoft-live-accountsvia-subdomain-hijacking/138719/ 4. *How can Office 365 phishing threats be addressed?:* https://www.helpnetsecurity.com/2018/05/18/office-365-phishing-threats/

8. 安全问题：控制面薄弱

从数据中心迁移到云，给创建足够的数据存储和保护。

历史排名
新的顶级威胁
安全责任
☑客户 ☒云服务提供商 ☒两者皆有
架构
☒应用架构 ☒信息架构 ☒元数据 ☑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)

计划带来了一些挑战。用户现在必须开发新的数据复制、迁移和存储流程—如果使用多云—情况会变得更加复杂。控制面应该是这些问题的解决方案，因为它实现了安全性和完整性，这将补充确保数据的稳定性和运行时间。薄弱的控制面意味着负责人—无论是系统架构师还是DevOps工程师—不能完全控制数据基础设施的逻辑、安全和验证能力。在这种情况下，利益相关者不知道安全配置、数据如何流动以及架构的盲点和脆弱点存在于何处。这些限制可能会导致数据损坏、不可用或泄漏。

业务影响

薄弱的控制面可能会因被窃取或损坏而导致数据丢失。这可能会导致巨大的业务影响，特别是在数据丢失中包括私人用户数据。还可能招致对数据丢失的监管处罚。例如，根据欧盟通用数据保护条例(GDPR)的规定，产生的罚款可能高达2000万欧元-或全球收入的4%。

在控制层面薄弱的情况下，用户也可能无法保护其基于云的业务数据和应用程序，这可能会导致用户对所提供的服务或产品感到沮丧和失去信心。最终，这可能会转化为收入的减少。

关键信息

1. 需要通过云服务提供商提供足够的安全控制，这样云客户才能确保合法和履行法定义务。
2. 云客户应进行尽职调查，并确定其要使用的云服务是否具有足够的控制面。

案例

最近与薄弱的控制面有关的问题包括：

•云服务的管理层面非常关键，需要通过身份和访问控制进行充分保护。双因素身份验证应该是云服务提供商提供给云客户的标准控制套件的一部分。不幸的是，许多云服务提供商只将双因素身份验证作为高级服务提供给他们的客户。这种做法削弱了云客户的安全状态-尤其是那些没有或不能使用这项高级服务的客户。

CSA 安全指南

领域1：云计算概念和体系架构。

领域5：信息治理。

领域7：基础设施安全。

领域8：虚拟化和容器 。

领域12：身份、授权和访问管理。

CCM 控制项

AIS 应用程序和接口安全

AIS-03：数据完整性

AIS-04：数据安全/完整性

AAC 审计保障与合规性

AAC-03：信息系统合规映射

BCR 业务连续性管理与运营恢复

BCR-04：文档化

DSI 数据安全与信息生命周期管理

DSI-04：处理/标示/安全策略

IVS 基础设施与虚拟化安全

IVS-01：审计日志/入侵检测

IVS-04：信息系统记录

IVS-06： 网络安全

IVS-09：隔离

IVS-13：网络架

GRM 治理与风险管理

GRM-01: 基线要求
GRM-02: 关注数据的风险评估
GRM-06: 策略
GRM-07: 策略实施
GRM-08: 风险评估对策略的影响
GRM-09: 策略评审
GRM-10: 风险评估
GRM-11: 风险管理框架

威胁分析	链接和引用
☒身份欺骗 ☑篡改数据 ☒抵赖 ☑信息泄露 ☒拒绝服务 ☑权限提升	1. *Uber fined $148m for failing to notify drivers they had been hacked:* https://www.theguardian.com/technology/2018/sep/26/uber-hack-finedriver-data-breach 2. *Exposed S3 bucket compromises 120 million Brazilian citizens:* https://www.scmagazine.com/home/security-news/exposed-s3-bucket-compromises-120-million-brazilian-citizens/

9. 安全问题：元结构和应用结构失效

云服务提供商通常会提供实施和保护其系统所必需的操作和安全保护措施。通常，云服务提供商会通过API接口公开此类信息，并且把保护措施合并到元结构中加以说明。元结构被认为是云服务提供商/云服务客户之间的分界线，也称为基准线。

历史排名
新的顶级威胁
安全责任
☒客户 ☒云服务提供商 ☑两者皆有
架构
☑应用架构 ☒信息架构 ☑元数据 ☒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)

在云计算模型中存在多个级别的故障可能性。例如，由云服务提供商引发的API实施不当，会为攻击者提供一些机会，如通过攻击导致云用户的服务中断，或破坏其机密性、完整性或可用性等。

为了提高云服务对客户的可见性，云服务提供商通常通过API接口提供在基准线上的安全流程交互。但是，不成熟的云服务提供商通常不确定如何向其客户提供API，以及在多大程度上提供API。例如，允许云服务客户检索日志或审计系统访问情况的API接口，可能包含高度敏感的信息。但是，这一过程对于云服务客户是非常必要的，用于检测未经授权的访问。

在基准线之上，云服务的客户必须了解如何正确实施和部署应用程序，充分利用云平台能力。例如，未充分考虑云环境下的要求而设计出来的应用程序，会因为与云环境无法互通，而没有利用云的资源和能力。将业务操作和应用程序迁移上云时，仅仅采用“提升和转移”方法是不够的。

业务影响

元结构和应用结构是云服务的关键组件。云服务提供商在这些功能上的故障可能会严重影响所有云服务的用户。同时，云租户的错误配置，可能会在财务和操作上对用户带来困扰。

关键信息

1. 云服务提供商必须提供可见性并公开缓解措施，以减轻因云对租户缺乏足够的透明机制而带来的影响。
2. 云租户应在云原生设计中实现适当的特性和控制措施。
3. 所有云服务提供商应进行渗透测试，并向云服务客户提供结果。

案例

与元结构和应用结构故障有关的事件案例：

- 关于元结构和应用结构失效，目前最一致的案例是围绕身份和访问管理问题发生的。许多组织仍然仅依靠用户名和密码，而忽略了在云中提供一些更易于实施的、全新的安全功能，例如单点登录（SSO），身份联合和多因素身份验证（MFA）。 例如，德勤（Deloitte）因泄漏了其在Office 365电子邮件服务的管理员帐户的密码（尽管Microsoft提供了MFA选项），结果，黑客破解了该帐户，从而暴露了大量的客户信息。
- Netflix是AWS最重的用户之一，了解元结构访问的重要性，并提供了在安全操作流程中对使用凭据泄露检测的步骤。 攻击者看到了元结构凭据的价值；微软警告说，以云凭据为目标每年的攻击持续增长。 根据2017年Microsoft安全情报报告，这些目标的攻击频率是上一年的三倍。 《 2018年Microsoft安全情报报告》的调查结果还表明，“ 79％ 的SaaS存储应用程序和86％的SaaS协作应用程序在静态存储和传输过程中都未对数据进行加密。”
- 一项 SecureWorks 对 AWS 社区市场的早期研究发现，超过一半的 AWS 镜像（机器镜像 AMI）被嵌入了缺陷。这些缺陷包括了临时目录中的文件、遗留在系统上的嵌入式密钥和遗留在快照上的其他运行级控制(rc)脚本。在不清楚镜像来源的情况下，镜像可能做出超出预期的行为。在这之后，（IaaS）提供商在各种市场上提供公开的说明和共享的要求。此外，应用结构的实施也存在类似的问题，苹果在 2019 年要求应用开发者删除录制应用程序界面活动以分析消费者行为的代码。

CSA 安全指南

领域1: 云计算概念和体系架构

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

CCM 控制项

AIS应用程序和接口安全
AIS-01: 应用程序安全
AIS-03: 数据完整性
AIS-04: 数据安全/完整性

AAC审计保障与合规性
AAC-01 : 审计策划

BCR业务连续性管理与运营恢复
BCR-02: 业务连续性的测试
BCR-04: 文档化

CCC变更控制和配置管理
CCC-01: 新开发/获取
CCC-05: 生产变更

DSI数据安全与信息生命周期管理
DSI-02: 数据目录/数据流
DSI-03: 电子商务交易
DSI-04: 处理/标示/安全策略
DSI-07: 安全处置

IAM身份与访问控制
IAM-01: 审计工具访问
IAM-02: 凭证生命周期/提供管理
IAM-04: 策略和规程
IAM-05: 职责分离
IAM-07: 第三方访问
IAM-08: 可信源
IAM-09: 用户访问授权
IAM-10: 用户访问评审
IAM-11: 用户访问撤销
IAM-12: 用户ID身份凭证
IAM-13: 实用程序访问

IVS基础设施与虚拟化安全
IVS-09: 隔离

EKM加密与密钥管理
EKM-02: 密钥生成
EKM-03: 敏感数据保护

HRS 人力资源安全
HRS-08: 技术可接受使用

SEF 安全事件管理，电子发现与云取证
SEF-03: 事件报告

IPY 互操作与可移植性
IPY-01: 应用程序接口

STA 供应链管理，透明与可审计
STA-03: 网络/基础设施

威胁分析	链接和引用
☑身份欺骗 ☑篡改数据 ☑抵赖 ☑信息泄露 ☑拒绝服务 ☑权限提升	1. *Why Cloud Security Is Everyone's Business:* https://www.gartner.com/smarterwithgartner/why-cloud-security-is-everyones-business/ 2. *Source: Deloitte Breach Affected All Company Email, Admin Accounts:* https://krebsonsecurity.com/2017/09/source-deloitte-breach-affected-allcompany-email-admin-accounts/ 3. *Deloitte hack hit server containing emails from across US government:* https://www.theguardian.com/business/2017/oct/10/deloitte-hack-hitserver-containing-emails-from-across-us-government 4. *Deloitte Gets Hacked: What We Know So Far:* http://fortune.com/2017/09/25/deloitte-hack 5. *"Get Off of My Cloud": Cloud Credential Compromise and Exposure:* https://www.defcon.org/images/defcon-19/dc-19-presentations/Feinstein-Jarmoc/DEFCON-19-Feinstein-Jarmoc-Get-Off-of-My-Cloud.pdf 6. *Netflix Cloud Security: Detecting Credential Compromise in AWS:* https://medium.com/netflix-techblog/netflix-cloud-security-detecting-credentialcompromise-in-aws-9493d6fd373a 7. *Microsoft Security Intelligence Report:* https://download.microsoft.com/download/F/C/4/FC41DE26-E641-4A20-AE5B-E38A28368433/Security_Intelligence_Report_Volume_22.pdf 8. *Microsoft warns that hackers are increasingly targeting cloud accounts:* https://www.theinquirer.net/inquirer/news/3016031/microsoft-warnsthat-hackers-are-increasingly-targeting-cloud-accounts 9. *Microsoft Security Intelligence Report volume 23 is now availablePoorly secured Cloud Apps:* https://cloudblogs.microsoft.com/microsoftsecure/2018/03/15/microsoft-security-intelligence-reportvolume-23-is-now-available/ 10. *Understand top trends in the threat landscape:* https://www.microsoft.com/sir 11. *What Is Amazon EC2?:* https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/building-shared-amis.htm 12. *Virtual machine prerequisites:* https://docs.microsoft.com/en-us/azure/marketplace/cloud-partner-portal/virtual-machine/cpp-prerequisites 13. *How to Log a Security Event Support Ticket:* https://docs.microsoft.com/en-us/azure/security/azure-security-event-suppor

	t-ticket 14. *Apple tells app developers to disclose or remove screen recording code:* https://techcrunch.com/2019/02/07/apple-glassbox-apps/ 15. *Announcing AWS CloudTrail:* https://aws.amazon.com/about-aws/whatsnew/2013/11/13/announcing-aws-cloudtrail/ 16. *AWS Discussion Forums - AWS CloudTrail Feature Additions:* https://forums.aws.amazon.com/forum.jspa?forumID=168 17. *AWS Discussion Forums - AWS CloudWatch Feature Aadditions:* https://forums.aws.amazon.com/forum.jspa?forumID=138 18. *Announcing the public preview of Azure Monitor:* https://azure.microsoft.com/en-us/blog/announcing-the-public-preview-of-azure-monitor/ 19. Azure AD Activity Logs in Azure Monitor Diagnostics now in public preview: https://techcommunity.microsoft.com/t5/Azure-Active-Directory-Identity/Azure-AD-Activity-Logs-in-Azure-Monitor-Diagnostics-now-in/ba-p/245435

10. 安全问题：有限的云使用可见性

当组织不具备可视化和分析组织内使用云服务是安全的还是非安全、不当的能力时，就会出现有限的云使用可见性。这个概念被分解为两个关键的挑战。未经批准的应用程序使用:当员工使用云应用程序和资源而没有获得公司 IT 和安全部门的特别许可和支持时，就会发生这种情况。

历史排名
新的顶级威胁
安全责任
☒客户 ☒云服务提供商 ☑两者皆有
架构
☑应用架构 ☑信息架构 ☑元数据 ☑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)

这个场景产生了一个名为影子 IT 的自我支持模型。当不安全的云服务活动不符合公司的指导方针时，这种行为是有风险的——尤其是在与敏感的公司数据配对时。

Gartner 预测，到 2020 年，三分之一成功的针对公司的安全攻击将来自影子 IT 系统和资源。

批准程序滥用：企业往往无法分析使用授权应用程序的内部人员是如何使用其已获批准的应用程序的。通常，这种使用在没有得到公司明确许可的情况下发生，或者由外部威胁行动者使用诸如凭证盗窃、SQL 注入、域名系统(DNS)攻击等方法来攻击服务。在大多数情况下，可以通过判断用户的行为是否不正常或是否遵守公司政策来区分有效用户和无效用户。

业务影响

这些风险广泛存在，但可以总结为以下几点：

- 缺乏治理：当员工不熟悉或未受过适当的访问和治理控制方面的培训时，经常会看到敏感的公司数据被放置在公共访问位置而不是私有访问位置。
- 缺乏意识:当数据和服务在公司不知情的情况下被使用时，他们本质上无法控制自己的 IP。员工拥有数据，而不是公司。
- 缺乏安全性：当员工错误地设置了云服务时，它不仅可以利用云服务上的数据，还可以利用未来的数据。恶意软件、僵尸网络、加密货币挖掘恶意软件等等都可以破坏云容器，从而使组织数据、服务和安全面临风险。

在《2019 年 Oracle 和 KPMG 云威胁报告》中，50%的受访者，当被问及未批准的云在各自的环境中使用的影响时,这种未经批准的使用导致了“未经授权的访问数据”,并另有 48%提到了“恶意软件的引入”。

关键信息

1.要降低这些风险，首先要从上到下开发一个完整的云可见性工作。这一过程通常是在组织的云安全架构师创建与人员、流程和技术相关的综合解决方案时开始的。下面概述的操作可以帮助快速启动这个过程。

2. 要求全公司范围内对公认的云使用策略及其实施进行培训。

3.所有未经批准的云服务都必须经过云安全架构师或第三方风险管理人员的审查和批准。

4. 投资于云访问安全代理(CASB)或软件防御网关(SDG)等解决方案，分析出站活动，帮助发现云使用情况、风险用户，并跟踪已获得证书的员工的行为使用情况，以识别异常情况。

5. 投资一个 web 应用防火墙 (WAF)来分析所有到您的云服务的入站连接，以发现可疑趋势、恶意软件、分布式拒绝服务(DDoS)和僵尸网络风险。

6. 选择专门设计用来监视和控制所有关键企业云应用程序(企业资源规划、人力资本管理、商业体验和供应链管理)的解决方案，并确保可以减轻可疑行为。

7. 在整个组织中实现零信任模型。

案例

最近关于有限的云使用可见性问题的例子包括：

- 根据云安全 frm Lacework 2018 年的研究:“超过 22000 个容器编排和 API 管理系统在互联网上是不受保护的或公开可用的——突出了云计算工作负载风险的现实。”
- Skyhigh Networks 2015 年第二季度云采纳与风险报告报告称，“目前企业平均使用 1083 项云服务。这一惊人的结果比去年同期几乎高出 50%，比两年前高出 100%。”
- 在目前使用的 1000 多个云服务中，Skyhigh Networks 2015 年第二季度的云采纳和风险报告称，许多服务可能属于影子 IT。简单地说:IT 部门在帮助选择和部署这些影子 IT 服务的服务方面没有任何作用，甚至可能不知道它们正在被使用。

CSA 安全指南

域 5: 信息治理

域 11: 数据安全和加密

CCM 控制项

DSI 数据安全与信息生命周期管理
DSI-01:分类
DSI-02: 数据目录/数据流
DSI-04: 处理/标示/安全策略
DSI-06: 责任人/管理者

EKM 加密与密钥管理
EKM-03: 敏感数据保护

GRM 治理与风险管理
GRM-02: 关注数据的风险评估

HRS 人力资源安全
HRS-03: 任用协议
HRS-07: 角色/职责
HRS-08: 技术可接受使用
HRS-09: 培训/意识
HRS-10: 用户职责

威胁分析	链接和引用
☑身份欺骗 ☑篡改数据 ☑抵赖 ☑信息泄露 ☑拒绝服务 ☑权限提升	1. 22K Open, Vulnerable Containers Found Exposed on the Net: https://threatpost.com/22k-open-vulnerable-containers-found-exposed-on-thenet/132898/ 2. Five Ways Shadow IT in the cloud hurts your enterprise: https://www.networkworld.com/article/2997152/cloud-computing/five-ways-shadow-itin-the-cloud-hurts-your-enterprise.html 3. Cloud Adoption and Risk Report: https://info.skyhighnetworks.com/WPCARR-Q2-2015_Download_White.html?Source=website&LSource=website 4. https://go.oracle.com/LP=79796?elqCampaignId=168050

11. 安全问题：滥用及违法使用云服务

恶意攻击者可能会利用云计算能力来攻击用户、组织以及云供应商，也会使用云服务来搭建恶意软件。搭建在云服务中的恶意软件看起来是可信的，因为他们使用了云服务商的域名。另外，基于云的恶意软件可以利用云共享工具来进行传播。其他滥用云资源的案例如：

- 启动DDoS攻击
- 垃圾邮件以及钓鱼邮件攻击
- 电子挖矿
- 大规模自动化点击犯罪
- 对账号服务器进行暴力攻击
- 存储恶意或盗版内容

历史排名
顶级威胁 10→顶级威胁 11
安全责任
☒客户 ☒云服务提供商 ☑两者皆有
架构
☑应用架构 ☑信息架构 ☑元数据 ☑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)

解决云服务滥用的办法包含云服务提供商检测支付漏洞及云服务的滥用。云服务提供商必须要建立事件响应框架，对这些滥用资源的行为进行识别并及时报告给客户。云服务提供商也需要采取相应的管控措施允许客户来监控其云负载及文件共享或存储应用程序的运行状况。

业务影响

一旦攻击者成功入侵客户的云基础设施管理平台，攻击者可以利用云服务来做非法事情，而客户还需要对此买单。如果攻击者一直在消耗资源，比如进行电子货币挖矿，那客户还需一直为此而买单。

另外，攻击者还可以使用云来存储和传播恶意或钓鱼攻击。公司必须要注意该风险，并且有办法来处理这些新型攻击方式。这可以包含对云上基础架构或云资源API调用进行安全监控。

关键信息

- 企业应该对使用云的员工进行监控，原来传统的机制不能解决云服务使用带来的风险
- 部署云上数据防泄漏（DLP）技术来监控和阻止任何非授权的数据泄露

案例

最近滥用及非法使用云资源的案例包含：

- 勒索软件Locky的变种Zepto 病毒利用微软OneDrive, Google Drive以及Box 文件分享功能来传播病毒
- CloudSquirrel攻击利用钓鱼邮件方式来攻击。攻击邮件诱使受害
- 者打开貌似重要的链接（比如发票），一旦打开，CloudSquirrel就会让受害者自动下载额外的加密恶意软件Java包，然后该恶意软件将会自动和Box的控制服务器建立联系，它的指令会通过明文文本文件来传递，但这些文件会以一个假的文件名存在，如mp4, WMV, PNG, data以及wma。

CSA 安全指南

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

CCM 控制项

AIS应用程序和接口安全
AIS-02: 客户访问要求

BCR业务连续性管理与运营恢复
BCR-09: 影响性分析

CCC变更控制和配置管理
CCC-02: 外包开发

DSI数据安全与信息生命周期管理
DSI-01:分类
DSI-02: 数据目录/数据流
DSI-04: 处理/标示/安全策略

EKM加密与密钥管理
EKM-03: 敏感数据保护

HRS人力资源安全
HRS -05：移动设备管理
HRS-08: 技术可接受使用
HRS-09: 培训/意识

IAM身份与访问控制
IAM-02: 凭证生命周期/提供管理
IAM-04: 策略和规程
IAM-05: 职责分离
IAM-09: 用户访问授权
IAM-10: 用户访问评审
IAM-11: 用户访问撤销
IAM-12: 用户ID身份凭证

IVS基础设施与虚拟化安全
IVS-01: 审计日志/入侵检测
IVS-02: 变更检测
IVS-06: 网络安全
IVS-13: 网络架构

GRM治理与风险管理
GRM-01: 基线要求

MOS移动安全
MOS-02: 应用程序商店
MOS-03: 授权的应用程序
MOS-04: BYOD的授权软件
MOS-05: 意识和培训
MOS-06: 基于云的服务
MOS-19: 安全补丁

TVM威胁、脆弱性管理
TVM-02: 脆弱性/补丁管理

威胁分析	链接和引用
☑身份欺骗 ☑篡改数据 ☑抵赖 ☑信息泄露 ☑拒绝服务 ☑权限提升	1. Malware Used by China APT Group Abuses Dropbox: http://www.securityweek.com/malware-used-china-apt-group-abuses-dropbox 2. Zepto variant of Locky ransomware delivered via popular Cloud Storage apps: https://resources.netskope.com/h/i/273457617-zepto-variant-oflocky-ransomware- delivered-via-popular-cloud-storage-apps 3. CloudSquirrel Malware Squirrels Away Sensitive User Data Using Popular Cloud Apps: https://resources.netskope.com/h/i/272453388-cloudsquirrelmalware-squirrels-away- sensitive-user-data-using-popular-cloud-apps 4. CloudFanta Pops with the Cloud using SugarSync: https://resources.netskope.com/h/i/295875750-cloudfanta-pops-with-the-cloud-usingsugarsync 5. Data Theft Via the Cloud: You Don't Need Flash Drives Any More: https://blog.learningtree.com/data-theft-via-cloud-dont-need-flash-drives/ 6. What Is Cloud DLP?: https://digitalguardian.com/blog/what-cloud-dlp 7. Best Practices for Cloud Security: https://insights.sei.cmu.edu/sei_blog/2018/03/best-practices-for-cloud-security.html

结论

随着云业务模型和安全策略的发展，本报告强调了对关键安全问题的认识，如数据泄漏、错误配置、身份和访问管理。其他威胁突出了用户在使用云服务供应商时可能遇到的缺乏控制的障碍，比如云使用中有限的可见性和薄弱的控制面。这些问题可能导致数据泄漏或超出传统范围的泄露，就像在过去的许多案例中所看到的那样。

考虑到用户界面和API是现在服务的使用方式，值得关注的是，在保护这些功能方面仍然存在重大挑战。

云本身非常复杂，同时也是攻击者隐藏的最佳场所。不幸的是，它也是一个理想的攻击起点。最后但并非不重要的一点是，内部威胁使保护组织免受数据丢失变得更具挑战性。

所有这些缺陷都需要更多的行业关注和研究。

这份云计算领域的顶级威胁报告为云安全提供了一个有趣且有点新颖的视角。这种新的观点关注配置和认证，而不是关注传统的信息安全(例如，漏洞和恶意软件)。无论如何，这些安全问题都需要继续完善以及对云安全意识、配置和身份管理的加强。

附录：方法论

在创建《顶级威胁 11 项: 2019 年云计算顶级威胁报告》时 CSA 顶级威胁工作组的研究包含两个主要阶段。并且两个阶段以调查和问卷作为主要研究工具。

在第一个研究阶段，工作的目标是创建一个云安全关注点候选清单。工作组从一个包含 26 项安全关注点的清单着手（对以前报告中的 12 项更新并增加了 14 项新关注点）。工作组通过一系列的会议对 26 项关注点进行了讨论，并要求成员们指出每一项的重要性。在这个研究阶段也同样给与工作组成员们对新增未包括在 26 项内的额外关注点的提议机会。综合以前调研结果和其他相关信息，工作组标定了 19 个最突出的云安全关注点。

在第二个研究阶段，工作的主要目标是通过重要性对上阶段标定的 19 项列表进行评级。工作组想要通过研究得到全专业人员角度最相关的云安全关注点，所以选择了 10 分滑动标尺作为研究工具。指导调研对象按照“1 至 10 分”对云安全问题进行评级打分，1 分代表非常不重要，10 分代表非常重要。对每项安全关注点得分计算平均值并进行排序。排除所有低于 7 分的安全关注点，最终得到了顶级威胁 11 项。

最后，工作组还使用微软的 STRIDE 威胁建模方法对安全关注点进行了分析。具体来说，就是将我们在本文档讨论的安全关注点按下表进行威胁分类:

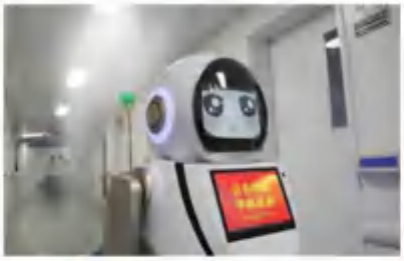
- 身份欺骗(S)
- 数据篡改(T)
- 抵赖(R)
- 信息泄露(I)
- 拒绝服务(D)
- 权限提升(E)

创泽智能机器人集团主要产品

智能服务机器人

智能陪护机器人

安防巡检机器人



消毒机器人

智能党建机器人

智能教育机器人

智能导诊机器人

银行智能机器人

室外智能消毒机器人

多功能消毒机器人

全自动智能消毒杀菌机器人

智能医用消毒机器人

了解更多登录官网

www.chuangze.cn

关于赞助者

ExtraHop 提供云原生网络检测和响应，以保护混合(云)企业。 我们的突破性方法将高级机器学习应用于所有云和网络流量，以提供完整的可见性、实时威胁检测和智能响应。 通过这种方法，我们为全球领先的企业（包括 Home Depot，瑞士信贷，Liberty Global 和 Caesars Entertainment）提供了他们需要超越（告警）噪声的视角来检测威胁、确保关键应用程序的可用性并保护他们在云中的投资。若需体验 ExtraHop 的强大功能，请浏览我们的交互式在线演示，或通过 LinkedIn 和 Twitter 与我们联系。