识别影子访问：新兴的IAM安全挑战

CSA GCR cloud security GREATER CHINA REGION alliance®

CSA cloud security alliance®

IAM工作组的官网地址是：

https://cloudsecurityalliance.org/research/working-groups/identity-and-access-management/

联盟简介

云安全联盟（Cloud Security Alliance,CSA）是中立、权威的全球性非营利产业组织，于2009年正式成立，致力于定义和提高业界对云计算和下一代数字技术安全最佳实践的认识，推动数字安全产业全面发展。

云安全联盟大中华区（Cloud Security Alliance Greater China Region, CSA GCR）作为CSA全球四大区之一，2016年在香港独立注册，于2021年在中国登记注册，是网络安全领域首家在中国境内注册备案的国际NGO，旨在立足中国，连接全球，推动大中华区数字安全技术标准与产业的发展及国际合作。

我们的工作

联盟会刊下载地址
了解联盟更多信息

加入我们

CSA大中华区官网
(https://c-csa.cn)

点击会员

加入联盟

填写相关申请信息

成为CSA会员

JOIN US

致谢

《识别影子访问：新兴的IAM安全挑战（Defining Shadow Access: The Emerging IAM Security Challenge）》由CSA IAM工作组家编写，CSA大中华区IAM工作组专家翻译并审校。

中文版翻译专家组（排名不分先后）：

组长：

于继万

翻译组：

崔崟　　于振伟　　鹿淑煜

审校组：

戴立伟　　谢琴

研究协调员：

蒋妤希

感谢以下单位的支持与贡献：

北京天融信网络安全技术有限公司　　华为技术有限公司

江苏易安联网络技术有限公司　　上海物盾信息科技有限公司

深圳竹云科技股份有限公司　　三未信安科技股份有限公司

在此感谢以上专家及单位。如译文有不妥当之处，敬请读者联系CSA GCR秘书处给予雅正！ 联系邮箱research@c-csa.cn； 国际云安全联盟CSA公众号。

英文版本编写专家

主要作者：

Sasi Murthy　　Venkat Raghavan　　Steven Schoenfeld

贡献者：

Philip Griffiths　　Shruti Kulkarni　　Michael Roza　　Dhaval Shah　　Heinrich Smit

审校者：

Ivan Djordjevic　　Rajat Dubey　　Ahmed Harris　　Senthilkumar Chandrasekaran

Shraddha Patil　　Alberto Radice　　Osama Salah

CSA分析师：

Ryan Gifford

编辑：

Larry Hughes

CSA全球员工：

Claire Lehnert

序言

在当今数字化时代，云计算技术的普及为组织带来了巨大的便利，然而，随着云计算的快速发展，一种新的安全挑战崭露头角：影子访问（Shadow Access）。影子访问指的是对资源、应用程序和数据的非有意或非预期的访问行为，其风险日益凸显，威胁着企业的数据安全和隐私保护。

本文深入剖析了影子访问现象，并指出了它对云计算、身份和访问管理、数据保护等多个方面的威胁和潜在影响。作为一个新兴的安全挑战，影子访问的影响远不止于数据的泄露，还可能破坏数据完整性与影响组织合规性。

为了更好地理解和应对影子访问，我们需要建立新一代的工具和流程，同时强调持续监控和自动化管理在解决这一问题中的重要性，以确保云环境访问与组织数据的安全。这不仅仅是一个技术问题，更是一个需要全面战略思考的挑战。

本文所指出的问题，正是当今企业面临的现实挑战。希望通过此白皮书的探讨和分析，引起广大企业对影子访问问题的关注，共同探讨解决之道，确保数字化时代信息安全的可持续发展。

李雨航 Yale Li

CSA 大中华区主席兼研究院院长

影子访问

影子访问指的是对资源、应用程序和数据的非有意或非预期的访问行为，这是随云计算、DevOps、云原生架构和数据共享的快速增长，而产生的一种新的安全问题。

影子访问越来越成为一个云问题，这是由于连接云服务的访问和授权使用增加，加上自动化的基础设施和软件开发，导致错误或者意外的账户和资源被配置。

从小发展到大的组织经常会痛苦地发现，曾经的安全起点会默默地演进到一个不安全的阶段。除了上述问题外，通常情况下，使用者的账号和权限会被克隆（典型场景是在员工入职或者新账号创建时），会为用户提供并非真正需要的访问权限，使影子访问问题进一步加剧。

影子访问的后果可能是灾难性的，并且可能威胁到正在向云演进的任何组织。这篇短文旨在总结影子访问的背景、原因、影响和前进的路径，以重获动态、安全的云环境所带来的益处。

背景

图 1: 企业IAM与云IAM的比较

传统的企业身份和访问管理（IAM）系统已经发展了数十年，通常通过 LDAP 或活动目录等典型服务或协议进行构建和部署。企业 IAM 为身份提供授权和凭证，通常将企业人力资源（HR）系统作为权威的身份数据源。围绕终端用户对应用和资源的操作调用和访问授权而建立起的策略和流程，通常被托管在企业防火墙内部，员工和承包商通过安全的 VPN 连接从防火墙外部进行访问。

随着云应用的显著发展，云身份提供者（IDP）系统开始出现。从定义上来看，云应用并不托管于企业内部。因此，目前许多企业采用了企业 IAM（用于本地部署的应用程序）和流行的云 IDP 相结合，如 Okta、Azure AD 或 Ping Identity。

云 IAM 是伴随云计算演进产生的一个新的概念，用于为云内资源、应用程序和数据提

供授权和访问控制，它们位于公有云生态系统中，如 AWS、Google 云和 Azure 云，以及由 Kubernetes 驱动的私有云。

虽然乍一看很相似，但在现实中，这个概念在本质上是不同的，因此，我们需要分别对这些云身份进行分类和检查。

那么，为什么会有一个叫做"云身份"的新概念以及它们有何不同？

- 无论访问云中的关键服务、供应链元素还是数据，每个资源都有一个身份。云服务提供商（例如 AWS、GCP 或 Azure）的系统通过像云 IAM 这样的关键服务，来控制所有资源的身份和访问。
- 云内的每个访问请求都经过身份验证和授权。
- 云身份可以是人类身份或非人类身份。人类身份主要包括终端用户、开发人员、DevOps 和云管理员。非人类身份占了绝大多数，包括与云服务、API、微服务、软件供应链、云数据平台等相关的身份。
- "可编程性"是云计算的强大能力之一，开发人员通过编程方式，组合云服务、API 和数据来创建应用程序。这是一个不容忽视的变化。现代云应用程序实际上是由通过 API 驱动的许多分布式服务组装而来，跨越了不同提供商的生态系统。当开发人员构建云服务时，他们创建了具有数据访问路径的自动身份。
- “自动化”是云计算的另一个强大之处。云团队使用“基础设施即代码”的自动化能力，来轻松地启动和定义云资源、云身份及其访问权限。自动化优先，治理其次。

云计算创造了一个以身份为中心的世界，围绕这些身份的差别正是产生"影子访问"的根本原因。

影子访问的根本原因

影子访问的根本原因不仅源于拥有云身份，还源于云环境中固有的复杂性和业务流程。

复杂性

上面提到的“云的强大能力”主要是通过开发人员和自动化发布的，而且比以前的环境要复杂得多。一些显著的差异包括：

- 数据不再储在单一存储中。跨云和 SaaS 环境中广泛分布着云端数据存储和数据共享应用。
- 全新或更新过的应用程序带来新的数据类型，数据存储因此不断演变，可能扩展亦或收缩。
- 应用程序不再是单体的，而是身份系统、云服务和数据等组件相互复杂连接产生的结合体。
- 与云端生态系统相关联的 SaaS 应用程序的使用量大幅增加。
- 每个云服务都有相关的权限，并有权利对敏感数据和操作进行授权。
- 与传统的本地环境相比，权限和授权的规模更为庞大，复杂度也高出几个数量级。
- 组织使用多云环境和公有云/私有云环境的组合。

为了说明这种复杂性，仅在 AWS 中就有 12,800 项云服务，附带 13,800 项权限，从而产生了巨大的云访问排列组合。

图2，引自https://aws.permissions.cloud/

流程变更

在以前的 IT 环境中，在创建身份并授予访问权限之前，通常会先实施严格的策略和流程。对于那些已经建立了访问控制的组织来说，身份的创建，以及始终如一的审查和批准过程通常都被纳入治理流程中。在这方面，云计算的运作非常不同：

- 新的身份和访问权限通常由使用基础设施即代码的开发人员集中创建。
- 新身份的配置文件通常是从一个模板复制过来的，并期望该模板通过了符合组织标准的集中审查程序。
- 新的身份和访问权限通常在几乎没有治理的情况下自动创建。
- 这些身份访问的应用程序持续迭代，却没有进行完全的访问审查。
- 为了加快效率，应用程序的各种组件经常被重用、复制或用于多个应用程序。
- 对没有正式安全审查的 SaaS 和第三方应用程序的使用越来越多。
- 应用程序访问的数据存储在不断变化。

持续监控、审查和权限调整需要和原始身份和访问权限创建一样实现自动化，但现实并

非如此。由于云应用是分布式的并且不断发展的，一个元素的变化可能对整体暴露产生意想不到的后果。

正是应用程序的高度复杂和不断演变的本质，以及围绕云身份创建和持续审查的流程的中断，导致了影子访问和一系列可能对组织造成巨大风险的潜在暴露。

影响

如前所述，影子访问指的是对资源、应用程序和数据的非有意或非预期的访问行为。

为了说明其影响，Verizon 数据泄露调查报告(DBIR)强调，80%的泄漏事件与身份和访问有关。云平台中存储了海量的数据（ZB 级），这推动了对访问控制的巨大需求。

影子访问的影响包括：

- 现有的工具无视云身份和访问路径的多样性。
- 治理和可见性的欠缺使实施 IAM 防护措施变得非常困难。
- 无法识别的访问路径导致漏洞可被利用来泄漏云数据。
- 攻击者能够将可编程访问武器化，造成的危害会远超数据泄露。
- 连接到云生态系统的第三方应用程序和 SaaS 应用程序会带来横向移动风险。
- 影子访问带来了数据安全、审计和合规风险，并造成了策略和治理的不足。

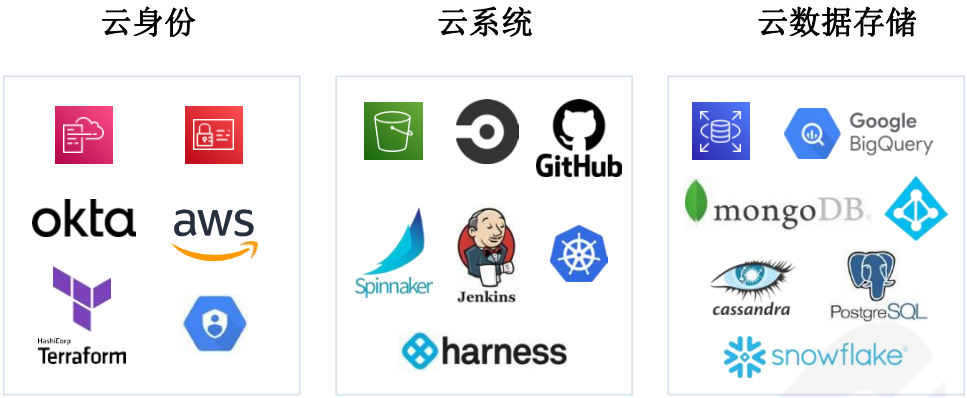

图 3. 影子访问存在于公有云生态系统（如，AWS）的多个系统中

本质上，环境的真正安全状态永远是未知的，在分析完成之前，获取信息的机制和过程通常已经过时。其结果是一个脆弱的环境，而环境的所有者没有办法真正评估风险。

> “在 CI/CD 生态系统中存在着成百上千个身份——包括人类和程序化身份——加上缺乏强有力的身份和访问管理实践，以及疏于管理的账户日常使用，导致了几乎在任何系统上攻击任何用户账户，都可能获得当前环境下的强大的能力，并可能成为进入生产环境的过渡。”
>
> 这段文字直接摘自 OWASP Top 10 CI CD SEC-2：
>
> https://owasp.org/www-project-top-10-ci-cd-security-risks/

结论

作为一种新现象，影子访问影响了云计算的多个领域。应对这个问题，需要建立并实施新一代的工具和流程，重新建立访问和数据安全的预期状态，以充分发挥云的优势。

关于理解影子访问的工作才刚刚开始。自动化、人工智能和数据的广泛应用形成了影子访问大量出现的基础土壤。它不仅影响访问，还影响更广泛的方面，如零信任。影子访问与零信任以及许多其他领域之间的关系将在未来的文件中更详细地讨论。

CSA GCR cloud security alliance
GREATER CHINA REGION

Cloud Security Alliance Greater China Region

扫码获取更多报告

云安全联盟大中华区
官网：https://c-csa.cn 电话：0755-86548359
地址：上海市浦东新区东育路255弄5号3FB30（前滩国际经济组织集聚区）/
广东省深圳市南山区粤海街道北京航空航天大厦1号楼905