从 PCI DSS 合规视角浅谈云租户环境的渗透测试

作者：atsec 高磊

关键词：云安全、云上租户环境、渗透测试、PCI DSS、CDE、责任矩阵、网络分段验证

atsec information security

Tel +86-10-53056681
Fax +86-10-53056678

www.atsec.com

目录

1 引言

随着企业逐步将支付业务系统、数据库、API 服务和运维组件部署至云环境，持卡人数据环境（CDE：Cardholder Data Environment）的边界也变得更加动态和复杂。相比传统数据中心，云环境具有资源弹性高、服务类型多、配置变化快等特点，但也带来了公网暴露面扩大、权限配置复杂、网络分段验证难度增加等安全挑战。

在企业进行 PCI DSS 合规时，选择具备 PCI DSS 合规能力的云服务商和相关云服务，可以为企业安全建设提供重要基础。但这并不意味着使用合规云平台的云租户自身也满足 PCI DSS 要求。在云环境中，云服务商与云租户之间通常存在明确的安全责任划分：云服务商主要负责云平台基础设施及相关托管服务的安全，云租户则需要对其在云平台上部署、配置、管理和使用的系统、数据、账号权限、网络访问控制和应用安全承担相应责任。在具体 PCI DSS 合规评估中，企业还应结合云服务商提供的责任矩阵（Responsibility Matrix），明确各项控制要求该由云服务商、云租户还是双方共同承担责任。

图 1：云环境责任矩阵示意图

根据 PCI DSS 11.4 相关要求，渗透测试不仅是合规评估中的重要验证活动，也可以从攻击者视角验证防火墙、网络分段、访问控制和应用防护等安全措施是否有效，帮助企业识别可能影响账户数据或 CDE 的真实攻击路径。因此，云环境下的渗透测试首先需要明确测试边界。本文所讨论的渗透测试并非针对云服务商底层基础设施、宿主机或云平台控制面的测试，而是聚焦于云租户自身拥有管理责任和测试授权的环境。而是聚焦“云上租户环境”，主要指云租户自身负责部署、配置、管理和使用的云上资产及相关安全控制，包括但不限于云主机、Web 应用、API 接口、数据库、中间件、对象存储、身份与访问管理（IAM：Identity and Access Management）权限、安全组、容器环境以及与 CDE 相关的网络分段边界。

2 云上租户环境渗透测试的必要性与价值

相比传统数据中心，云环境中的资产创建、变更和释放更加灵活，云主机、公网 IP、负载均衡、对象存储、数据库实例、API 网关等资源可能随着业务变化快速调整。这种灵活的弹性提升了业务效率，但同时也使攻击面更加动态，安全组开放过宽、对象存储权限配置不当、云数据库暴露公网、IAM 权限过大、访问密钥管理不当等配置类问题，都可能成为攻击者进入云上环境或影响 CDE 的路径。

从标准要求来看，PCI DSS 11.4 对内部和外部渗透测试提出了相关要求：在使用网络分段降低 CDE 范围时，也需要验证分段控制的有效性。因此，云上租户环境的渗透测试不仅是 PCI DSS 合规评估中的重要验证活动，也是形成合规证据的重要依据。从安全保障角度来看，渗透测试可以从攻击者视角验证防火墙、网络分段、访问控制、应用防护和云配置等安全措施是否有效，帮助企业识别可能影响账户数据或 CDE 的真实攻击路径。

从 PCI DSS 合规视角来看，渗透测试的价值不只是发现传统意义上的系统漏洞或应用漏洞，更重要的是验证云上安全控制是否真正有效。虽然云服务商提供的 PCI DSS 合规证明（AOC：Attestation of Compliance）可以作为评估云平台合规能力的重要依据，但其通常只能证明云服务商在特定服务和范围内满足相关合规要求，并不能保证租户在云上的部署、配置和使用方式同样安全。

因此，云租户仍需通过针对性的渗透测试，从攻击者视角验证自身云上资产的外部攻击面是否可控、访问控制是否合理、云配置是否存在高风险，以及 CDE 与非 CDE 环境之间的隔离措施是否真正切断了非授权的访问路径。通过此类验证，企业可以识别真实攻击路径，确认现有安全控制的有效性，并为后续整改和持续合规提供依据。

3 云上租户环境执行渗透测试的主要关注点

在云环境的渗透测试中，测试重点不应局限于传统网络端口或单一应用漏洞，而应进一步关注云配置错误、身份权限缺陷和网络分段不足是否可能形成真实攻击路径，并验证其是否会影响云上关键资产或 CDE 访问边界。

3.1 云上业务暴露面与应用安全测试

云上业务系统同样面临 OWASP Top 10 等常见漏洞威胁。因此，云上渗透测试仍需覆盖传统网络层和应用层测试内容，对公网暴露的资产、管理入口、业务系统和 API 接口进行基础验证，识别可能被攻击者用于获得初始访问入口的风险点。同时，由于云上应用往往与云服务深度集成，单个应用漏洞可能进一步影响云端权限、存储资源或 CDE 访问边界，因此测试时还应关注漏洞可能形成的后续攻击路径。

图 2：针对云上租户执行渗透测试范围示意图

3.2 不同部署形态下的测试关注点

在实际 PCI 渗透测试项目中，云上业务服务器可能采用虚拟机、Docker 容器或 Kubernetes 集群等不同部署形态。部署方式不同，渗透测试的关注点也会有所差异。对于传统云主机或虚拟机部署的业务系统，测试思路与传统服务器较为接近，重点通常包括操作系统和中间件加固、端口暴露、弱口令、补丁版本、远程管理入口以及安全组访问控制等内容，但仍需结合云平台的公网暴露面、路由表和访问控制策略进行综合判断。

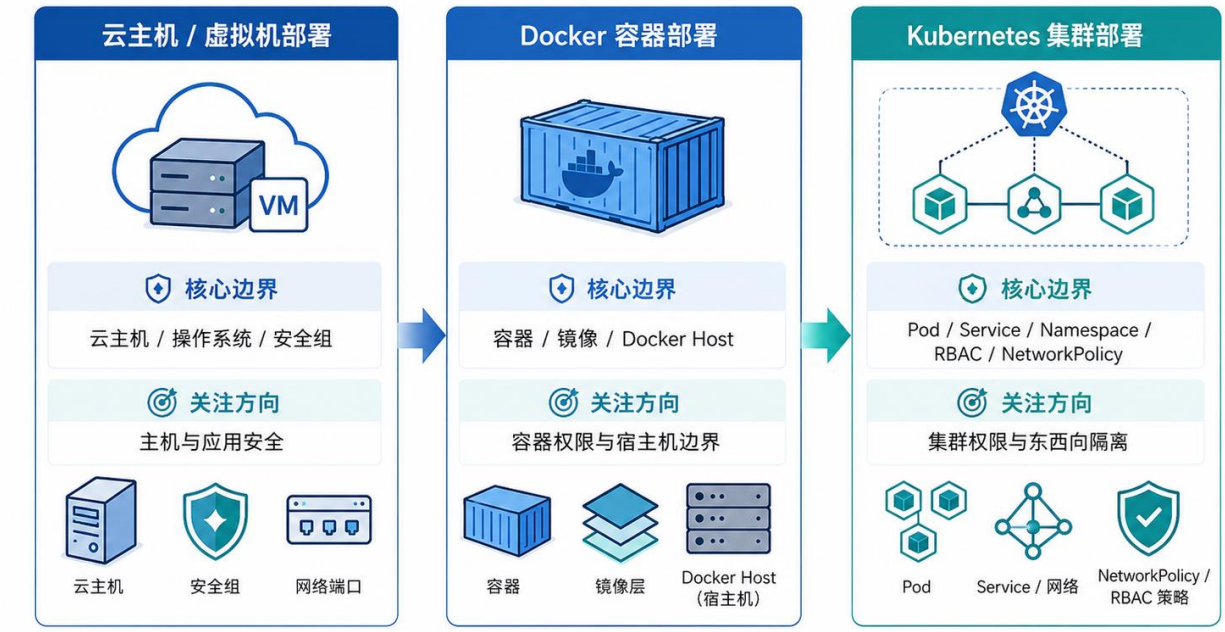

图 3：不同部署形态下的渗透测试边界变化示意图

对于 Docker 或 Kubernetes 等容器化部署环境，测试人员除关注应用本身漏洞外，还应进一步关注镜像安全、容器运行权限、敏感目录挂载、环境变量中的敏感信息、Secret 管理、ServiceAccount 权限、基于角色的访问控制（RBAC：Role-Based Access Control）配置以及容器网络策略等问题。如果容器运行权限过高、宿主机敏感目录被不当挂载，或集群内权限控制配置不当，单个应用漏洞可能进一步影响容器宿主机、集群资源或同一集群内的其他业务组件。以下为不同部署形态下渗透测试的主要关注点：

部署形态	主要测试关注点
云主机/虚拟机	操作系统和中间件加固、端口暴露、弱口令、补丁版本、远程管理入口、安全组访问控制
Docker 容器	镜像安全、容器运行权限、敏感目录挂载、环境变量敏感信息、Docker 管理接口、容器端口暴露
Kubernetes 集群	ServiceAccount 权限、RBAC 配置、Secret 管理、Ingress/API Server 暴露、NetworkPolicy、命名空间隔离

表 1：不同部署形态下的主要测试关注点

在 PCI DSS 场景下，还需要关注容器化环境对 CDE 网络分段验证带来的影响。部分非 CDE 业务容器与 CDE 相关容器可能运行在同一集群或相邻网络环境中，其隔离效果不仅依赖传统的虚拟私有云（VPC：Virtual Private Cloud）、安全组和路由表，也可能依赖 Kubernetes NetworkPolicy、命名空间、RBAC 和服务访问控制等逻辑隔离措施。因此，测试人员需要结合实际部署形态，验证非 CDE 工作负载是否能够访问或影响 CDE 相关服务，避免因容器平台配置不当导致分段控制失效。

3.3 云配置与身份权限安全测试

相比传统环境，云环境中的误配置更容易形成攻击路径。包括但不限于：安全组开放过宽、数据库或管理端口暴露公网、对象存储桶公开访问、访问密钥泄露、IAM 权限过大、高权限账号未启用多因素认证（MFA：Multi-Factor Authentication）、云审计日志未开启等问题，都可能导致攻击者滥用云端权限或访问敏感资源。

在云环境中，身份与权限往往是新的安全边界，测试人员除验证外部可访问的服务和端口外，还应重点关注访问密钥是否泄露、账号和角色权限是否过大、低权限账号是否可以通过云 API 访问高敏感资源，以及关键操作是否具备有效的审计记录。对于涉及 CDE 的云上环境，还应进一步判断相关配置或权限缺陷是否可能影响 CDE 访问边界。

3.4 云存储访问控制与数据暴露风险测试

对象存储、文件存储、快照、镜像、数据库备份和日志归档中，可能保存业务数据、配置文件、接口日志或敏感凭证。由于这类资源通常与业务系统、运维流程和备份机制紧密相关，一旦访问控制配置不当，容易造成敏感信息暴露或合规范围扩大。

测试人员应验证相关存储资源是否存在匿名访问、权限过宽、共享链接不当开放、敏感文件泄露、未加密存储等问题。并关注备份、快照、镜像和日志中是否包含账号密钥、数据库连接信息、接口凭证或业务敏感数据。对于支付场景，还需要关注持卡人数据或敏感认证数据是否被错误存储在非 CDE 范围内，从而导致合规范围扩大或数据泄露风险增加。

3.5 分段有效性验证（Segmentation Verification）

CDE 与非 CDE 环境之间的网络分段验证，是 PCI DSS 标准 11.4.5 的要求，是合规场景下云上渗透测试的重点之一。云环境中的分段边界通常由虚拟私有云（VPC：Virtual Private Cloud）、子网、安全组、路由表、访问控制列表（ACL：Access Control List）、云防火墙、堡垒机、VPN、跨账号访问关系等多种控制共同构成。

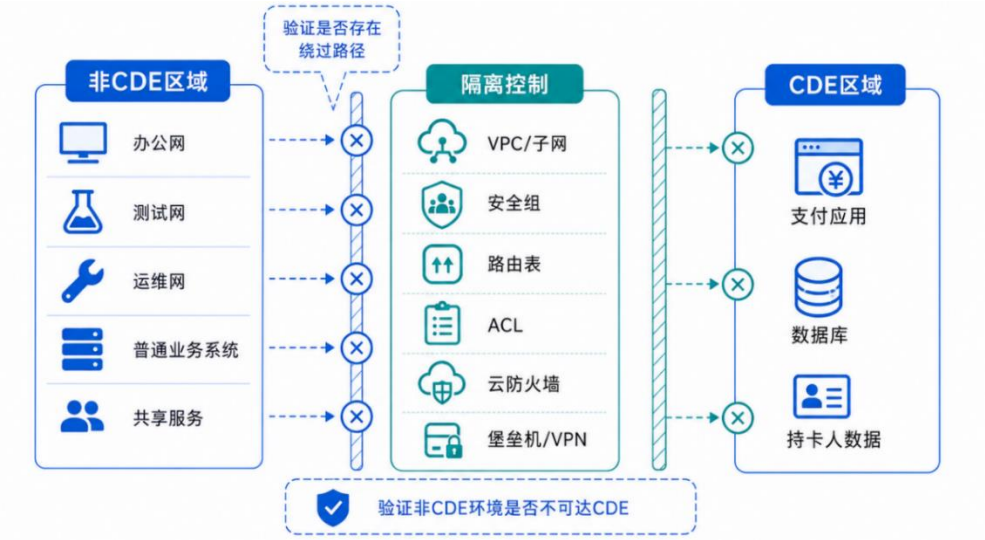

图:4：CDE 网络分段有效性验证示意图

测试人员应从攻击者视角验证办公网、测试网、运维网、普通业务系统或共享服务是否可以直接或间接访问 CDE，确认非 CDE 环境在实际攻击路径上无法绕过隔离措施影响 CDE。并关注是否存在通过管理通道、共享服务、跨账号授权、容器网络或临时放行规则绕过分段控制的可能。对于发现的可达路径，应进一步判断其是否可能影响持卡人数据环境的安全边界，确认非 CDE 环境在实际攻击路径上无法绕过隔离措施影响 CDE。

总的来说，定期检查网络隔离有效性，不光是满足支付合规的硬性规定，还能在网络上建起一道防护墙。云平台隔离规则复杂，各类临时开通、跨账号互通的后门很容易留下漏洞，只有持续测试查漏补缺，才能守住敏感数据，避免泄露带来罚款和经营风险。

4 测试结果的整改闭环与持续治理

合规不是安全工作的终点，而是云安全运营的基础。云上渗透测试的价值不应只停留在发现漏洞，更应体现在帮助企业识别真实攻击路径，并推动后续整改和安全能力提升。

首先，企业应基于测试结果建立闭环整改机制。对于能够直接影响 CDE 的高风险问题，应优先修复，并在整改完成后进行复测，确认相关漏洞和攻击路径已被有效修复或阻断。

其次，企业应从测试发现中反推防御加固方向。例如：

- 针对 IAM 滥用风险，应进一步排查云上账号、角色、策略和访问密钥，推动权限最小化原则落地；
- 针对安全组、对象存储、数据库暴露等高频问题，应形成符合自身业务特点的云安全配置基线，减少同类问题反复出现。

在多次 PCI 渗透测试实践中，同类问题往往会在不同系统、不同云账号或不同部署环境中重复出现，例如安全组开放过宽、测试环境与生产环境隔离不足、对象存储权限配置不当、访问密钥管理不规范、容器环境敏感信息泄露等。因此，企业应将单次测试发现沉淀为可复用的检查规则、整改模板和云安全基线，使渗透测试结果真正转化为长期安全治理能力。

最后，云环境资源变化快，容易因业务变更、临时授权或运维操作产生配置漂移。因此，企业应将单次渗透测试中发现的问题转化为持续监测规则，对云上资产的变化情况等进行持续验证，逐步形成“发现—整改—复测—监控”的安全闭环。

5 结论

在云环境下，渗透测试具有安全验证和合规支撑的双重价值。它不仅可以帮助企业满足 PCI DSS 对渗透测试和分段验证的相关要求，更重要的是通过攻击者视角，检验云租户自身资产、配置、身份权限和隔离架构的有效性。

云服务商的合规能力可以为企业提供重要基础，但无法替代云租户自身对业务系统、数据、权限和网络边界的安全管理责任。企业只有在责任边界清晰、资产范围明确、安全控制有效、测试验证充分的基础上，才能更好地保护持卡人数据，并持续提升云环境中持卡人数据的保护能力和安全运营水平。

A 参考文献

[1] PCI Security Standards Council. Payment Card Industry Data Security Standard: Requirements and Testing Procedures, v4.0.1. 2024.

[2] PCI Security Standards Council. Information Supplement: Penetration Testing Guidance, v1.1. 2017.
https://www.pcisecuritystandards.org/documents/Penetration-Testing-Guidance-v1_1.pdf

[3] PCI Security Standards Council. Information Supplement: PCI SSC Cloud Computing Guidelines, v3.0. 2018.
https://www.pcisecuritystandards.org/pdfs/PCI_SSC_Cloud_Guidelines_v3.pdf

[4] PCI Security Standards Council. Information Supplement: Guidance for PCI DSS Scoping and Network Segmentation, v1.1. 2017.
https://www.pcisecuritystandards.org/documents/Guidance-PCI-DSS-Scoping-and-Segmentation_v1_1.pdf

[5] OWASP Foundation. Web Security Testing Guide, v4.2.
https://owasp.org/www-project-web-security-testing-guide/v42/

[6] OWASP Foundation. OWASP Top Ten Web Application Security Risks. 2025.
https://owasp.org/www-project-top-ten/

[7] OWASP Foundation. Cloud Security Testing Guide.
https://github.com/OWASP/www-project-cloud-security-testing-guide