运维安全中心（堡垒机）

产品简介

腾讯云

文档目录

产品简介
产品概述

最近更新时间：2025-08-26 18:04:32

概述

运维安全中心（堡垒机）（Operation and Maintenance Security Center（Bastion Host））是集用户（Account）管理、授权（Authorization）管理、认证（Authentication）管理及综合审计（Audit）于一体的集中运维管理系统，提供 IT 资产访问代理以及智能操作审计服务，为用户构建一套完善的事前预防、事中监控、事后审计安全管理体系，实现异常行为告警，防止内部数据泄密，助力企业开展等保测评。
运维安全中心（堡垒机）主要特点：

- 为企业提供集中的管理平台，减少系统维护工作。
- 为企业提供用户和资源管理功能，降低企业维护成本。
- 帮助企业制定严格的资源访问策略，并且采用强身份认证手段，保障系统资源安全。
- 详细记录用户对资源的访问及操作，达到对用户行为审计的需要。

产品功能

运维安全中心（堡垒机）能够审计多种主流运维协议，对服务器、操作系统运维工作进行详尽记录，确保企业安全问题得到有效追溯。

认证管理

运维安全中心（堡垒机）可以根据用户场景的实际需要，为不同用户提供不同类型的认证方式，既支持基本的静态口令方式，又能够集成现有认证方式（例如： 轻量级目录访问协议（LDAP））。同时，为了提高安全性，运维安全中心（堡垒机）支持用户使用双因子认证方式，实现用户认证的统一管理。

授权管理

运维安全中心（堡垒机）能够集中管控用户访问资产的权限，不仅能够实现对资产的访问权限的控制，还能够实现对操作命令、剪切板、文件传输的细粒度控制。基于最小权限原则进行授权，确保用户拥有的权限是其访问资产、完成工作任务所需要的最小权限。

资产访问

运维安全中心（堡垒机）支持托管 IT 资产的账号密码，运维人员可单点登录到目标资产进行运维操作，无需记忆全部资产的账号密码，仅需记住自己运维安全中心（堡垒机）账号和密码即可。

操作审计

运维安全中心（堡垒机）能够对用户操作日志进行记录和分析，不仅可以对用户行为进行监控，还可以通过集中的审计数据进行数据挖掘，以便于事后进行安全事故责任的追溯和认定。

产品优势

最近更新时间：2025-08-26 18:04:32

全面的资产管理

支持多云、线下资产的统一管理，支持主流的 Linux 操作系统、Windows 操作系统和 MySQL 数据库版本，有效辅助管理员进行安全运维。

细粒度权限控制

支持基于用户、资产、账号、操作权限等维度进行细粒度授权，确保用户所拥有的权限是企业客户所需的访问资产、完成工作任务的最小化权限。

良好的运维体验

支持多种主流运维操作客户端工具，并且适配 Windows 和 macOS 终端，运维过程当中，不改变运维人员原有的操作习惯。

运维操作审计

对运维人员访问服务器的操作命令、传输文件和运维过程进行审计，确保安全事件有效追溯。

统一运维入口

运维安全中心（堡垒机）作为统一的入口进行内部资产的管理和维护，用户无需记忆多个地址和多套账号密码。

异常风险告警

从时间、命令语句、下载/上传操作、访问 IP、服务器、用户名等多个维度进行分析，将异常行为筛选并告警，确保内部恶意事件提前有效预防。

应用场景

最近更新时间：2025-08-14 17:33:52

互联网+业务

互联网+业务云上资源众多，大量运维服务暴露在公网，且由于服务高度公开，容易被外部攻击者盯上。
运维安全中心（堡垒机）在业务资源远程运维时，通过隐藏真实运维端口与真实管理账户，解决远程运维安全问题。同时产品提供云上服务器运维日常审计，通过运维规则库梳理不良运维习惯，减少运维事故，帮助业务系统长期稳定运行。

企业

企业内部通常存在大量经营数据等敏感信息，这些信息在行业中具有一定价值，且容易泄密。
运维安全中心（堡垒机）为账号与岗位进行细粒度的权限划分，确保运维人员无法越权操作。

金融

金融行业具有大量金融数据及个人信息，且存在大量第三方代维机构，代维机构是否违规操作是金融企业需要重点关注的一个问题。 运维安全中心（堡垒机）为账号与岗位进行细粒度的授权控制，严格落实岗位规范，确保运维人员无法越权操作。通过 AI 引擎对运维行为进行深度分析，挖掘内部异常操作，防止数据被非法利用。

政务民生

政务民生在互联网化过程中，需要大量第三方机构进行建设和运维。
运维安全中心（堡垒机）可将运维方与管理方的权责分明，通过操作审计对运维问题进行追溯，确保安全事故有效定责。通过 AI 引擎对运维行为进行深度分析，挖掘内部异常操作，对民生政务数据（医疗、教育、社保、税务等信息）泄露进行预警。

SaaS 型运维安全中心（堡垒机）与传统型堡垒机的区别

最近更新时间：2024-06-19 14:17:31

运维安全中心（堡垒机）型号

运维安全中心（堡垒机）目前仅提供 SaaS 型产品，相比传统型堡垒机，SaaS 型运维安全中心（堡垒机）采用分布式架构，提供云原生的产品服务。

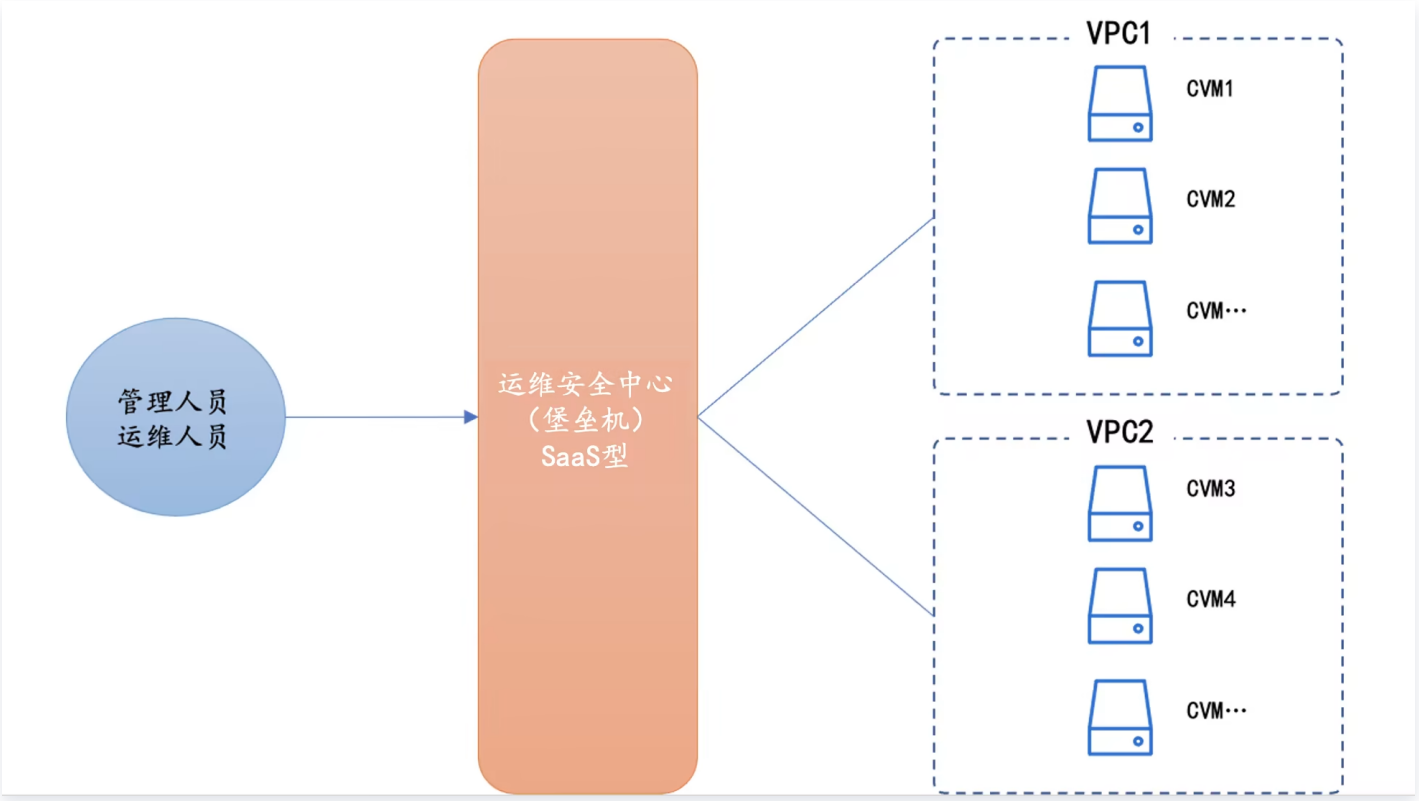
类别	SaaS 型运维安全中心（堡垒机）	传统型堡垒机
技术架构	分布式架构，SaaS 服务	单机软件，支持双机热备
部署方式	即开即用，无需安装部署	需要购买云服务器 CVM，安装软件镜像
核心优势	• 可弹性升级、扩容 • 可集中纳管不同私有网络 VPC 中的 CVM • 与腾讯云深度集成，自动同步腾讯云资产	功能覆盖度高

说明

一个运维安全中心（堡垒机）SaaS 服务最多可绑定一个VPC，通过 SaaS 型运维安全中心（堡垒机）纳管不同 VPC 中的资产可参考实践教程 跨 VPC 资产管理 。

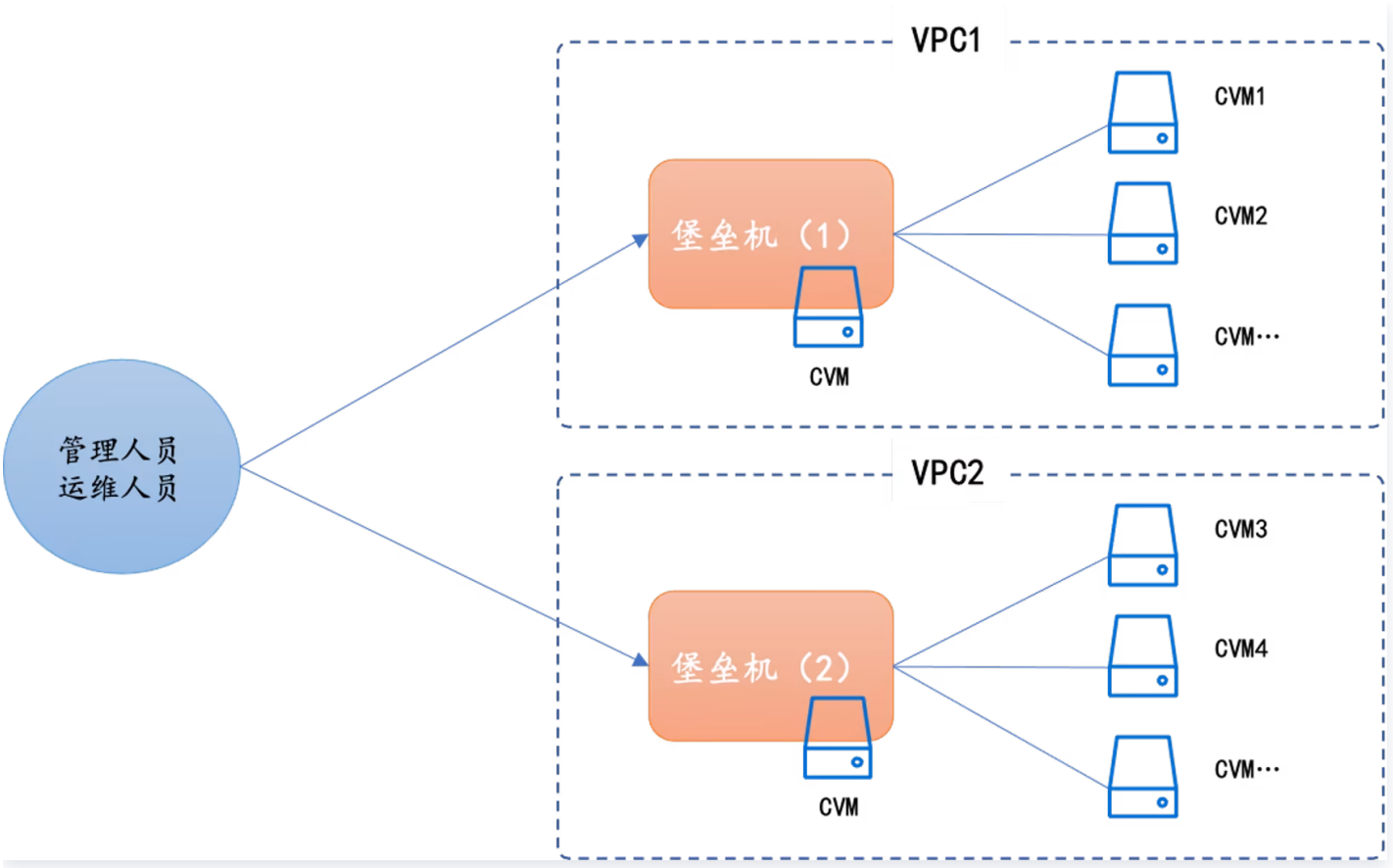
SaaS型运维安全中心（堡垒机）

SaaS型运维安全中心（堡垒机），部署过程对租户完全透明，且不占用租户资源。能够对不同 VPC 中的 CVM 进行集中纳管，为租户提供即开即用、弹性扩容的 SaaS 化服务。



传统型堡垒机

传统型堡垒机，是把堡垒机镜像安装到租户 VPC 指定的 CVM 上，实现对该 VPC 中其他 CVM 的纳管，不同 VPC 中需要安装多套软件。


VPC1
CVM1
堡垒机（1）
CVM2
CVM…
CVM
管理人员
运维人员
VPC2
CVM3
堡垒机（2）
CVM4
CVM…
CVM

运维安全中心（堡垒机）版本区别

最近更新时间：2025-11-05 09:58:21

运维安全中心（堡垒机）提供了基础版、专业版和国密版三个版本，本文将详细介绍三个版本之间的差异。

- 专业版：适用于有等保测评、数据库资产纳管需求，或关注运维效率提升的企业。
- 基础版：适用于对云服务器有基本运维、审计需求的中小型企业。
- 国密版：适用于对信息安全和合规性要求较高的各类企业。

产品版本区别

功能项	功能描述	基础版	专业版	国密版
规格配置	支持选购的产品规格	• 50 资产 • 100 资产 • 200 资产 • 500 资产	• 50 资产 • 100 资产 • 200 资产 • 500 资产 • 1,000 资产 • 2,000 资产 • 5,000 资产 • 10,000 资产	• 50 资产 • 100 资产 • 200 资产 • 500 资产 • 1,000 资产 • 2,000 资产 • 5,000 资产 • 10,000 资产
资产管理	支持数据库资产管理	仅支持 MySQL	✔	✔
	支持主机资产管理	✔	✔	✔
	支持容器资产管理	×	✔	✔
	支持应用资产管理	×	✔	✔
	支持资产账号自动改密和账号推送	×	✔	✔
自动运维	支持对多台主机进行批量操作，提升运维效率	×	✔	✔

操作审计	支持数据库操作日志记录	×	✔	✔
	支持主机运维操作日志记录	✔	✔	✔
	支持文件传输操作日志记录	✔	✔	✔
国密通信	用户登录堡垒机运维页面时，支持国密登录认证。国密 HTTPS 不仅能够提供强大的安全保护，还能够尽可能确保信息传输符合国家标准和政策要求	×	×	✔
国密认证	用户登录堡垒机运维页面时，支持国密登录认证。国密认证在保障信息安全、符合国家法规、增强信任、自主可控等方面具有显著的优势，是提升信息系统安全性和可靠性的关键手段	×	×	✔

说明：
基础版提供了 MySQL 数据库资产管理功能，帮助用户可以体验到专业版的数据库资产管理能力。专业版和国密版支持的数据库可参考 添加数据库资产 。

标配带宽

规格	基础版	专业版	国密版
50 资产、100 资产、200 资产	8 Mbps	16 Mbps	8 Mbps
500 资产、1000 资产、2000 资产	16 Mbps（仅支持 500 资产）	32 Mbps	16 Mbps
5000 资产、10000 资产	–	64 Mbps	32 Mbps

高可用性

运维安全中心（堡垒机）通过多代理节点方式保障产品的高可用性，其中：基础版 500 资产规格支持多代理节点，专业版和国密版所有规格均支持多代理节点。

说明：
基础版 50、100、200 资产规格仅支持单代理节点。