

行云管家堡垒机 东莞行云管家堡垒机 企业信息安全管理

产品名称	行云管家堡垒机 东莞行云管家堡垒机 企业信息安全管理
公司名称	广东蓝讯智能科技有限公司
价格	.00/个
规格参数	
公司地址	东莞市南城街道周溪隆溪工业区隆溪路10号金汇科技园A238
联系电话	18028990096

产品详情

随着企业信息化建设步伐的不断加速，IT对企业业务起到的支撑作用也越来越明显，毫不夸张地说，在相当一部分企业中，IT已经发展成为企业的生命线。相应地，在现如今信息安全事故频发的背景下，企业对内部信息安全的管控要求也越为严苛。

传统模式下，企业会考虑通过部署堡垒机的方式来提高企业内部信息安全管理水平，提供控制和审计依据，并满足相关法规要求。这些措施在传统运维方式下并无大碍，但在已经到来的云计算时代，企业已经开始逐步采用并充分利用云计算的低成本、按需配置等核心优势来满足企业的弹性化IT需求。云计算的发展将会对企业的信息安全带来新的挑战，主要体现在：传统的运维模式与管理思维是否能够适应云的变化？如何确保混合云模式下的统一管理与安全运维？是否能够充分发挥云计算好的优势？

行云管家总结多年IT领域的实践经验，用互联网思维并基于互联网与云计算架构自主研发的一体化云计算管理平台，行云管家堡垒机是其核心功能。通过行云管家堡垒机，可对私有云、公有云等计算资源进行运维、监管与审计，并实现账号集中管理、双因子认证、访问授权控制等功能让企业内部人员、第三方代维人员的操作处于可见、可管、可控、可审的状态，规范运维的操作流程避免误操作和非法授权带来的安全隐患降低安全风险，满足合规性要求，并保障企业IT的安全、可持续运行。

一、企业内部自身的诉求

数据表明，70%以上的IT故障其实都是人为引起的，这意味着信息化安全管理首先要解决的是加强内部信息安全管理。针对企业内部IT运维管理，我们经常需要思考的问题是：你是谁？你的身份是否合法？你能访问哪些设备？你对设备拥有哪些权限？你正在设备上做怎样的操作？一旦产生非法操作或者误操作，是否能够做到回溯追责？通过对国内外数百家企业IT运维管理的调研，我们认为，企业内部IT运维管理现状普遍存在以下问题：

1、账号密码管理不规范

随着企业IT规模的不断增大，各类主机资源、应用系统的管理也变得愈加困难，这些资源往往都有一套

独立的账号体系，为了方便管理，企业管理人员通常会用一个简单的表格来记录这些信息操作人员的日常运维管理也存在多人共用账号的情况。多人共用账号在带来方便性的同时，账号本身的安全性无法得到保证，导致操作者的身份无法确定，当系统发生问题后，很难确认具体责任人。为了保证密码的安全性，企业通常会制定严格的服务器密码管理策略，诸如密码必须定期修改，密码需保证足够的强度等，但现实中，由于管理的资源规模太大和账号数量太多，这一费时费力的操作，往往都无法真正落地。

2、资源授权不清晰

在对资源进行授权管理时，如果仅依靠操作系统或应用系统本身的授权体系来实现管理，这样的方式过于粗放，尤其是在账号密码的管理本身就不规范的情形下，如果再缺少资源层面的授权策略，无法基于小权限分配原则管理用户权限，将导致难以与业务管理要求相协调。

3、访问控制不严格

访问控制的目的是通过限制运维人员对数据信息的访问能力及范围，保证信息资源不被非法使用和访问。企业目前的运维操作流程类似一个“黑盒”，我们并不清楚运维人员：

你是谁？

在访问哪台服务器？

正在服务器上进行哪些操作？

执行的操作是否合规？

4、缺乏有效的运维审计能力

在现今信息安全事故频发的背景下，对于运维人员的操作，如果缺乏有效的运维审计能力，一旦出现运维事故时，我们很难进行回溯追责。如果简单的依赖于系统日志，由于系统日志可读性差、零散、可删除、可篡改、并且账号与运维人员无法一一对应，所以这并不是一种有效的审计方式。

二、外部政策法规的要求

随着网络安全风险的增大，近年来业界安全事件层出不穷。为了加强信息管理，政府、金融监管部门、运营商等均发布了相关信息安全管理法规和要求。其中，《网络安全法》、《信息安全等级保护管理办法》、《商业银行信息科技风险管理指引》、《塞班斯法案》等法规均对信息管理提出了内控与运维审计的明确要求。

三、面临云计算特别是公有云的冲击

云计算不再是什么大势所趋，而是既成事实。诸多企业都已将IT系统迁移至云环境中，其中包括企业自建私有云及阿里云、腾讯云、Amazon等厂商提供的公有云服务。

云计算技术的发展使得传统IT的运维方式发生了相当程度的变化，诸如混合云管理、公有云产品的安全防护等等。在传统的IT环境中，安全边界非常明确，我们可以利用传统堡垒机、防火墙等对服务器、应用系统进行严格的访问控制，在业务迁入公有云环境后，传统堡垒机、防火墙已经不再适用，业务的边界远不如传统IT环境边界清晰，因此在云环境下，运维安全问题显得更加突出面临的运维安全形势更加严峻。

四、行云管家堡垒机设计理念

行云管家堡垒机是以4A管理理念为设计基础，满足国家相关堡垒机产品法规的要求，为用户提供合规的账号体系、严格的认证机制、完善的授权模型、运维审计的一款堡垒机产品。它采用纯软件形态设计，通过B/S的形式进行管理，实现对IT运维过程进行全面监管，做到有效的事前预防、事中监管及事后审计，满足用户的安全管理需求。

与传统堡垒机产品不同的是，传统堡垒机是在用户与IT资产之间建立了一套“运维审计系统”，而行云管家堡垒机承担的职责远不止于此。在满足4A管理理念的同时，为了降低堡垒机对运维工作的影响，行云管家堡垒机将用户与IT资产进行分离，将自身定位为“运维中枢”、“会诊平台”、“黑匣子”三位一体的堡垒机平台，以保障运维工作的高效、提升故障处理水平、满足运维审计的要求。