SANGFOR
深信服科技

深信服运维安全管理系统
堡垒机 OSM-1000 V3.0 白皮书

深信服科技股份有限公司

2019 年 06 月 04 日

版权声明

免责条款

本文档仅用于为最终用户提供信息，其内容如有更改，恕不另行通知。

深信服科技股份有限公司在编写本文档的时候已尽最大努力保证其内容准确可靠，但深信服科技股份有限公司不对本文档中的遗漏、不准确、或错误导致的损失和损害承担责任。

信息反馈

如果您有任何宝贵意见，请反馈至：

地 址：深圳市南山区学苑大道 1001 号南山智园 A1 栋

邮 编：518055

电 话：0755-86627888

传 真：0755-86627999

您也可以访问深信服科技网站：www.sangfor.com.cn 获得最新技术和产品和方案信息。

目 录

1 概述

客户总是问这么两个问题：如何有效管理我们的内网运维？如何有效避免运维安全事故？“如何有效管理我们的内网运维”是管理问题，“如何有效避免安全责任事故”是技术问题。如何有效地协调技术和管理从而提高运维安全和效率就成了我们必须要解决的问题。

如何有效管理我们的内网运维？

首先，我们内网的运维人员是谁？（企业内聘的维护人员？厂商的驻场人员？第三方的代维人员？）。这些运维人员在内网中的安全级别、管理权限各不相同，如何有效的加以区分？

其次，我们管理的内网设备都包括什么？（服务器？交换设备？安全中间件？数据库？防火墙？）。这些设备都采用什么操作系统？使用什么通信协议？使用那些连接工具进行访问？

按照等级保护的基本要求，为了避免单一管理员权限过高，需要把运维管理的权限划分为三部分，也就是运维管理“三员”（系统管理员、安全保密管理员、安全审计员）。三员之间彼此独立，相互监视，相互制约。如何有效划分运维三员？

明确了以上几点，那么内网管理问题其实可以归结为如下内容：

1) 明确管理人员真实身份；
2) 内网资源的注册和注销；
3) 自然人与内网资源的授权关系管理；
4) 运维“三员”权限划分和如何有效实现三员独立。

如何有效避免运维安全事故？

内网中常见的运维责任事故包括核心业务数据泄露、误操作导致核心业务中断、断网、恶意攻击、植入木马等。

解决上述问题的关键在于如何实现有效的运维审计。

1) 如何将审计记录精确定位到自然人而不是系统账号，从而有效地实现抗抵赖；

2) 如何统一审计日志格式；

3) 提供方便的可查询的审计记录；

4) 审计具有有效的时间戳；

5) 审计不可更改或删除；

6) 审计日志应全程完整记录运维用户的运维操作。

我们的思路

我们的最初的想法很简单，那就是在运维人员和目标设备之间架设一台管理设备。使用类似于网页代理的方式代理用户的运维协议。运维人员必须通过运维安全管理系统登录目标资源。这样我们就可以对用户的真实身份进行统一管理。同时可以管理目标资源到用户的权限映射（也就是授权管理）。最后，由于运维人员的完整运维流都是由运维安全管理系统代理的，所以运维安全管理系统可以通过视频录像的方式完整的记录用户运维行为的全过程，可以在一定程度上实现访问控制。

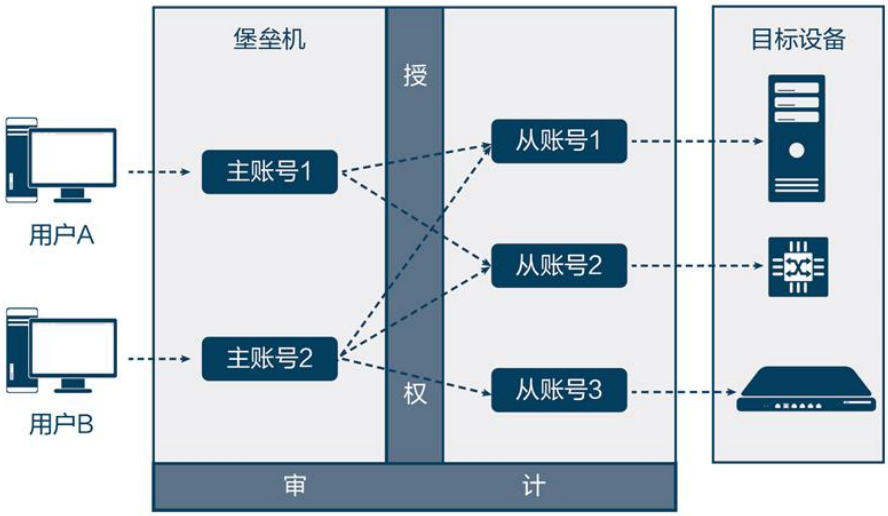

图 1.1 堡垒机工作原理图

2 需求背景

目前用户对 IT 系统的依赖程度也越来越高，各类业务系统也变得日益复杂。就一个信息化程度很高的网络信息系统而言，其针对传统的信息安全问题防护，已经比较完善，最大的威胁和破坏来自用户内部。据调查，8.5%的安全问题导致

网络数据破坏，11%的安全问题导致数据失密，23%的病毒程序感染问题导致系统短暂故障，而从恶意攻击的特点来看，70%的攻击来自组织内部。

在所有内部隐患中，一种由 IT 系统“权贵”人员及其操作引出的非传统的安全隐患日益凸显，是所有安全事件中最主要的安全威胁。所谓 IT 系统“权贵”人员，即拥有用户内网各种 IT 系统软硬件设备管理权限的人员，这些人员可能包括：系统管理员、系统运维人员、系统应用高权限用户、第三方厂商的维护人员以及其他临时高权限人员等。这些人员本身所拥有的高权限账号和其在操作过程中的各种动作，都带来日益明显的安全隐患。

近年来，国家对于政府机构及大型支撑企业的运维安全管理越来越重视，公安部颁发的《网络安全等级保护基本要求》、保密局颁发的《涉密信息系统的分级保护基本要求》中都对运维审计和访问控制做了严格要求。

随着信息化的发展，企事业单位 IT 系统不断发展，网络规模迅速扩大，设备数量激增，建设重点逐步从网络平台转向深化应用、提升效益为特征的运维阶段；IT 系统运维与安全管理正逐渐走向融合。面对日趋复杂的 IT 系统，不同背景的运维人员已经给用户信息系统安全运行带来较大的潜在风险，因此，内网信息系统安全治理在加大网络边界防护、数据通信安全、防病毒等基础上，不能忽略网络后台运维安全治理和对于系统操作人员的审计监控方面的管理，而运维安全管理系统作为内网安全治理的一种有效技术手段应运而生。

2.1 法规标准要求

2.1.1 等级保护

公安部等四部委《网络安全等级保护基本要求》

序号	控制域	控制项	控制条款	运维安全管理系统对应功能项
1.	8.1.3 安全区域边界	8.1.3.5 安全审计	a) 应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	运维安全管理系统部署在关键服务器运维区域的网络边界或入口，将用户对服务器的操作审计信息从日志级别提升到事件级别。
2.			b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计	运维安全管理系统的运维审计记录包括用户、开始时间、结束时间、运维协议等，图

序号	控制域	控制项	控制条款	运维安全管理系统对应功能项
			相关的信息；	形协议包括键盘记录、窗体识别，字符协议包括命令详情、执行结果等。
3.			c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；	运维安全管理系统安全审计员可以定期备份、定期删除审计记录信息；运维审计具有导入、导出功能。
4.	8.1.4 安全计算环境	8.1.4.1 身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	运维安全管理系统可对登陆用户进行身份标识和鉴别，确保身份标识具有唯一性，口令可设定复杂度和更换周期，满足身份鉴别安全策略要求。
5.			b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	运维安全管理系统用户登陆可配置登陆失败锁定处理，在非法访问一定次数后进行锁定处理；并可配置会话超时策略，登陆控制台指定时间误操作后自动注销会话。
6.			c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听；	运维安全管理系统对目标服务器发起运维操作时采用一次性会话号机制进行连接加密，确保鉴别信息不被窃听。
7.			d) 应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。	运维安全管理系统拥有本地认证、AD 域认证、Radius 认证、数字证书认证，提供外部接口可供指纹识别认证、UKEY（移动数据证书）认证。
8.		8.1.4.2 访问控制	a) 应对登录的用户分配账户和权限；	运维安全管理系统为登陆用户分配主账号，且访问权限由相应管理员赋予。
9.			b) 应重命名或删除默认账户，修改默认账户的默认口令；	运维安全管理系统支持默认初始化用户注销功能，且支持配置用户初次登陆修改密码机制防止默认口令带来的隐患。
10.			c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	运维安全管理系统安全管理员可对用户账号进行管理，可删除多余的、停用的、过

序号	控制域	控制项	控制条款	运维安全管理系统对应功能项
				期的、离职的账号，并可在建立用户时指定账号有效期，过期自动锁定。
11.			d) 应授予管理用户所需的最小权限，实现管理用户的权限分离；	运维安全管理系统内置三员账号，三权分立且只有角色必须权限，且与服务器运维操作员角色权限互斥，确保权限最小化。
12.			e) 应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则；	运维安全管理系统通过主从账号一一对应的授权方式，赋予用户完成操作的最小权限。其中命令访问控制策略，能对高危命令进行告警或阻断；文件传输控制策略可以对文件的上传/下载进行控制，达到允许或阻止的能力。访问控制粒度达到文件或命令级别。
13.			f) 访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级；	
14.			g) 应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。	
15.		8.1.4.3 安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	运维安全管理系统能够对字符、图形、数据库操作、WEB 应用等各类操作进行审计；字符类审计能不仅可以命令识别，而且还可以对命令执行结果进行记录；图形类审计能够实现实时的文字识别功能，完成标题栏的识别、精准定位；数据库操作能够实现协议解析，完整无死角进行操作审计；WEB 应用等的安全审计，让整个信息系统的任何操作都逃避不了运维安全管理系统的“法眼”，并能根据客户需求输出各类可查询的审计记录；运维安全管理系统作为独立的第三方审计系统，可以有效避免数据遭到破坏或非授权的访问删除、增加、篡改；对于审计记录只审计员可以查看，并实现三权分立的原则；并
16.			b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	
17.			c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；	
18.			d) 应对审计进程进行保护，防止未经授权的中断。	

序号	控制域	控制项	控制条款	运维安全管理系统对应功能项
				为安全管理中心提供接口，输出日志等相关信息。
19.		8.1.4.4 入侵防范	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制。	运维安全管理系统可设定 IP 地址规则以及时间规则限制可登陆的管理终端地址以及可管理用户的时间范围。
20.	8.1.5 安全管理中心	8.1.5.1 系统管理	a) 应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计；	运维安全管理系统身为一套独立的运维安全管理系统，其系统管理由单独的系统管理员角色在身份鉴别后在特定管理页面完成，且每个操作均有日志记录。
21.		8.1.5.2 审计管理	a) 应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计；	运维安全管理系统身为一套独立的运维安全管理系统，其审计管理由单独的审计管理员角色在身份鉴别后在特定管理页面完成，且每个操作均有日志记录。
22.			b) 应通过审计管理员对审计记录应进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。	运维安全管理系统审计管理员可对日志记录进行分析、生成报表等操作，且可以根据安全审计策略查询和备份审计数据。
23.		8.1.5.3 安全管理	a) 应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计。	运维安全管理系统身为一套独立的运维安全管理系统，其安全管理操作由单独的安全管理员角色在身份鉴别后在特定管理页面完成，且每个操作均有日志记录；安全管理员对安全策略的配置包括密码策略等安全参数的设置，授权策略可配置主体、客体，并可配置访问审批、主副岗审核等可信验证策略。
24.			b) 应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等。	
25.		8.1.5.4 集中管控	b) 应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理。	运维安全管理系统的安全的运维通道可以实现网络设备、安全设备的运维管理，形成有效的安全集中管控平台。

序号	控制域	控制项	控制条款	运维安全管理系统对应功能项
26.	8.1.10 安全运维管理	8.1.10.6 网络和系统安全管理	a) 应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限；	运维安全管理系统内置系统管理员、安全管理员、安全审计员三个角色，实现三权分立、各司其职。
27.			e) 应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容；	审计管理：运维审计内记录运维用户操作资源系统的行为；配置审计内记录管理员配置运维安全管理系统的相关操作；
28.			f) 应指定专门的部门或人员对日志、监测和报警数据等进行分析、统计，及时发现可疑行为；	运维安全管理系统的安全管理员可配置告警策略，且接收告警信息，同时可对告警归纳中的告警信息进行分析处理，审计员可以对日志信息进行分析和报表导出。
29.			g) 应严格控制变更性运维，经过审批后才可改变连接、安装系统组件或调整配置参数，操作过程中应保留不可更改的审计日志，操作结束后应同步更新配置信息库；	运维安全管理系统可对敏感服务器或者高危操作配置访问审批和命令策略，改变连接、安装系统组件或者调整配置参数等高危操作需要在审批后才可执行，并生成不可更改的审计记录。
30.			h) 应严格控制运维工具的使用，经过审批后才可接入进行操作，操作过程中应保留不可更改的审计日志，操作结束后应删除工具中的敏感数据；	运维安全管理系统可以实现运维管理人员的身份认证和授权管理，只有认证成功的运维管理人员才可通过运维安全管理系统使用指定工具访问授权的资源，也就是特定的被管资源分配给特定的用户去运维，保证了操作工作和操作范围的安全可控。操作结束后不会在运维工具中保留任何数据，保障了敏感数据的安全。并且提供多级访问审批、命令运维审批以及双人授权功能，可实现被赋予运维权限的用户也需要在特定条件和审批流程下才可以进行运维操作。

序号	控制域	控制项	控制条款	运维安全管理系统对应功能项
31.			i) 应严格控制远程运维的开通，经过审批后才可开通远程运维接口或通道，操作过程中应保留不可更改的审计日志，操作结束后立即关闭接口或通道。	运维安全管理系统可配置对于远程运维开通需要特定用户审批，待审批通过后才能使用远程运维。同时审计日志中记录用户远程运维相关的操作行为。
32.	8.工业控制系统安全扩展要求 8.5.4 安全计算环境	8.5.4.1 控制设备安全	a) 控制设备自身应实现相应级别安全通用要求提出的身份鉴别、访问控制和安全审计等安全要求，如受条件限制控制设备无法实现上述要求，应由其上位控制或管理设备实现同等功能或通过管理手段控制。	运维安全管理系统可作为控制设备的上位控制或管理设备部署，实现身份鉴别、访问控制和安全审计等安全要求，拟补安全控制设备条件限制导致的不符合安全策略的现状。

2.1.2 行业法规

财政部、审计署、证监会、银监会、保监会联合颁布的《企业内部控制基本规范》

该规范的关键点是如何把 IT 内控与企业内控管理统一起来，信息安全审计则成为企业 IT 内控、安全风险管理的不可或缺的技术手段。

萨班斯.奥克斯利法案（Sarbanes-Oxley）

该法案强调企业的信息技术策略和系统中的内部控制，以及对审计过程存档的要求，即企业的内控活动（不论是人还是机器）的操作流程都必须明白地定义并保存相关记录。

2.2 管理现状

目前信息化运维管理有以下三个特点：

- 关键的核心业务都部署于 Unix 和 Windows 服务器上；
- 应用的复杂度决定了多种角色交叉管理；
- 运行维护人员更多的依赖 Telnet、SSH、FTP、RDP 等进行远程管理。

基于这些现状，在运维管理中存在以下突出问题。

2.2.1 账号管理方面存在安全隐患

- **IT 运维外包**

IT 运维外包带来了一定效率的提高，但企业无法直接有效管理外包人员，无法对外包人员的操作行为做到有效地控制和监管，甚至无法确保外包人员不会破坏或窃取企业设备、数据。

目前，越来越多的企业选择将非核心业务外包给设备商或代维公司，在享受便利的同时，由于代维人员流动性大、对操作行为缺少监控带来的风险日益凸显。

- **设备口令管理**

为了保证密码的安全性，安全管理员制定了严格的密码策略，比如密码要定期修改，密码要保证足够的长度和复杂度等，但是由于管理的机器数量和帐号数量太多，往往导致密码策略的实施流于形式。或者多台设备设置相同的密码，或者干脆把所有密码以明文的形式记录在某个文档中，这都给密码的安全性带来了威胁。

2.2.2 授权管理风险

- **人为管理运维权限存在风险**

随着行政事业单位及企业系统、网络规模的扩大，设备的增多，设备管理人员也会相应的增多；由于运维用户角色及设备功能的不同，存在数据中心人员、分支机构、代维厂商等多种角色，操作人员管理分散，多点登录，同时这样的人为交叉管理会造成运维用户可能的违规操作和越权访问，并且无法实现有效的监管。

- **缺乏细粒度访问授权**

大多数企事业单位的 IT 运维均采用设备、操作系统自身的授权系统，授权功能分散在各设备和系统中。管理人员的权限大多是粗放式的管理，缺少统一的运维操作授权策略，授权粒度粗，无法基于最小权限分配原则管理用户权限。因此，出现运维人员权限过大、内部操作权限滥用等诸多问题，如果不及时解决，信息系统的安全性难以充分保证。

2.2.3 认证管理漏洞

- **运维人员需要记忆大量从帐号、口令**

IT 系统中通常部署了大量的网络设备、主机系统和应用系统，分别属于不同的部门和不同的业务系统，各应用系统都有一套独立的帐号体系，运维人员需要记忆权限范围内的所有设备、系统的系统帐号、口令，容易造成：口令强度不足、口令单一、输错口令等。

- **设备认证手段单一**

目前大多数的终端登录、业务应用登录都实现了强身份认证，如 usb-key、CA 证书、动态口令等，而对服务器的运维管理往往缺少强认证的手段，这是由于某些网络设备、系统不支持强认证系统的改造，或改造成本较高。

2.2.4 审计管理方面

- **海量日志分散且格式不一**

各系统独立运行、维护和管理，所以各系统的审计也是相互独立的。各系统的日志格式、内容不一致，对日志信息的提取大多要依靠管理员的技术水平来决定。

- **基于源 IP 的审计无法定位到自然人**

大多数的安全审计产品，只能审计到时间、源 IP、系统帐号名称等信息，但不能标识出具体是哪个自然人访问了服务器，导致发生安全事件后，无法准确定位责任人。

- **镜像类审计产品对加密及图形协议束手无策**

常见的网络审计产品，采用的是镜像抓包的方式进行分析审计，但是对 SSH、等加密协议以及 RDP 等图形协议的运维协议无法做到内容解析，无法有效的解决运维人员操作审计的问题。

- **缺乏有效的运维监控手段**

目前现有的主机审计、网络审计产品仅仅只能实现事后的审计作用，但是对运维人员的操作内容无法做到实时监控、没有访问控制策略进行实时控制。

3 产品概况

3.1 产品定位

运维和审计管理平台，将运维人员离散维护主机及网络设备的行为统一到该平台进行，加强对系统安全以及运维的控制力。一方面通过集中运维，减少因离散操作导致的失误，提高工作效率，如新的安全策略在主机上的统一应用等；另一方面通过对所有用户在主机上的操作行为进行监控与记录，实时了解用户的操作行为，发现风险及时中止用户的操作，并记录下用户所有的操作行为，便于进行事后的审查与取证。

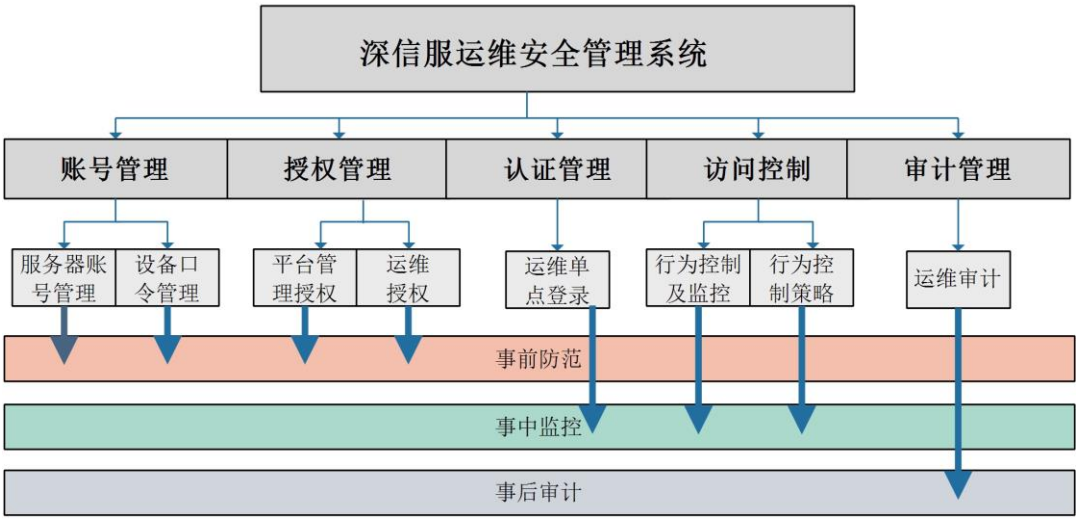

图 3.1 产品功能

3.2 运维安全管理系统关键技术说明

运维安全管理系统采用一系列先进技术，成功实现命令及图形的捕获与控制，为服务器的安全运行提供了强有力的系统工具。

3.2.1 逻辑命令自动识别技术

运维安全管理系统自动识别当前操作终端，对当前终端的输入输出进行控制，组合输入输出流，自动识别逻辑语义命令。系统会根据输入输出上下文，确定逻辑命令编辑过程，进而自动捕获出用户使用的逻辑命令。该项技术解决了逻辑命令自动捕获功能，在传统键盘捕获与控制领域取得了新的突破，可以更加准确地控制用户意图。

该技术能自动识别命令状态和编辑状态以及私有工作状态，准确捕获逻辑命令。

3.2.2 图形协议代理

为了对图形终端操作行为进行审计和监控，运维安全管理系统对图形终端使用的协议进行代理，实现多平台的多种图形终端操作的审计，例如 Windows 平台的 RDP 方式图形终端操作，Linux/Unix 平台的 VNC 方式图形终端操作。

3.2.3 多进程/线程与同步技术

运维安全管理系统主体采用多进程/线程技术实现，利用独特的通信和数据同步技术，准确控制程序行为。多进程/线程方式逻辑处理准确，事务处理不会发生干扰，这有利于保证系统的稳定性、健壮性。

3.2.4 数据加密技术

运维安全管理系统在处理用户数据时都采用相应的数据加密技术来保护用户通信的安全性和数据的完整性，防止恶意用户截获和篡改数据，充分保护用户数据在操作过程中不被恶意破坏。

3.2.5 审计查询检索技术

自从《萨班斯法案》推出，企业内控得到了严格的审查，企业的内部审计显得非常重要。

运维安全管理系统能够为企业内部网络提供完全的审计信息，这些审计信息能够为企业追踪用户行为，判定用户行为等，能够还原出用户的操作行为。

传统审计关联到 IP，这本身是一个不确定的和不负责任的审计结果，因为 IP 信息不能够真实反应出真实的操作者是谁，从而导致企业内部网络出现问题不能追踪到操作者。运维安全管理系统能够对这些用户行为进行关联审计，就是说真正能够把每一次审计出的用户操作行为绑定到自然人身上，便于企业内部网络管理追踪到个人。

3.2.6 操作还原技术

操作还原技术是指将用户在系统中的操作行为在真实的环境中模拟显现出来，审计管理员可以根据操作还原技术还原出真实的操作，以判定问题出在哪里。

运维安全管理系统采用操作还原技术能够将用户的操作流程自动地展现出来，能够监控用户的每一次行为，判定用户的行为是否对企业内部网络安全造成危害。

4 产品架构与性能

4.1 产品架构

4.1.1 逻辑架构

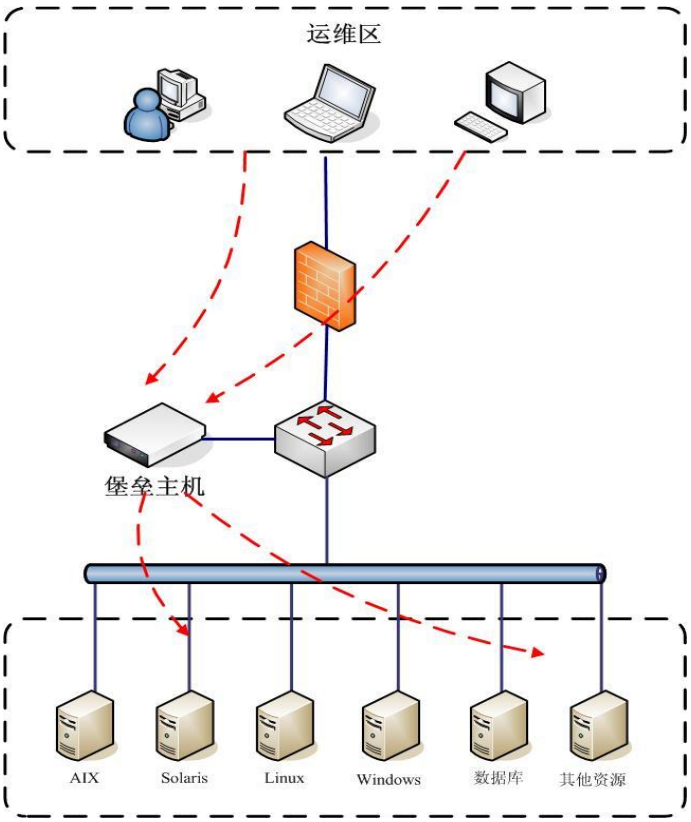

图 4.1 逻辑部署图

逻辑构架说明：

运维安全管理系统物理上以旁路的方式部署在运维终端与被管理设备之间的交换机上，逻辑上以串行的方式部署在运维终端与被管理设备之间。用户在访问被管理设备时，要先登录运维安全管理系统，通过运维安全管理系统以协议代理的方式访问被管理设备。运维安全管理系统根据登录用户的角色和权限，在 Portal 上显示用户可以访问的被管理设备列表，再通过单点登录功能登录到用户要访问的设备，用户的操作行为受到运维安全管理系统的访问控制和审计。

4.2 工作原理

运维安全管理系统由展现层、核心服务层、接口管理层三层组成。

展现层集成多种强身份认证服务；分别对系统管理员、运维 SSO 用户两类用户提供不同的访问操作页面。

核心服务层用于完成账号管理、授权管理及策略设置等操作；其中的协议代理包含用户输入模块、命令捕获引擎、策略控制和日志服务。

接口管理层用于实现审计结合、账号同步、认证结合等方面的数据接口工作。另外也包含应用发布服务，应用发布服务可以实现对 B/S、C/S 系统的单点登录及审计工作。

系统整体架构图如下：

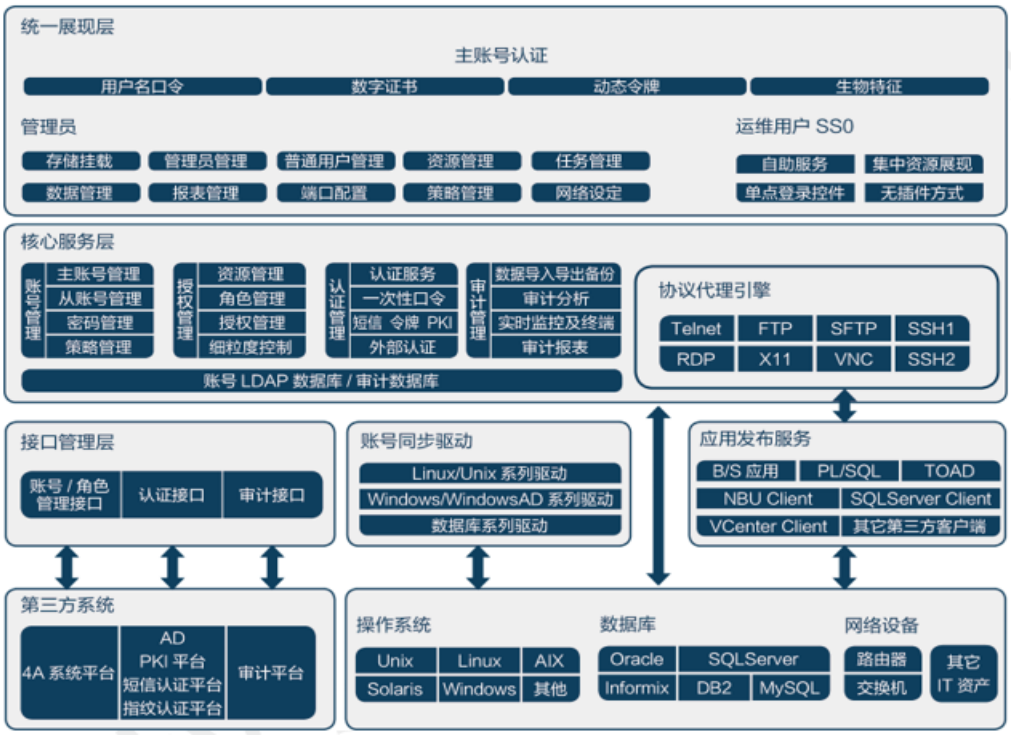

图 4.2 系统架构

核心服务层负责完成命令的采集、策略动作执行等功能。核心服务层安装在服务器上，同用户使用环境和习惯相配合，完成对用户行为的监视与控制功能。

- 统一账号管理

管理员通过主账号信息管理界面维护主账号的整个生命周期，对主账号进行增加、修改、删除及锁定、解锁等操作，同时设置主账号的密码使用策略及用户的级别定义。

主账号用户可以通过个人信息维护功能来管理自身账号信息，对手机、邮件及密码等个人信息进行修改。

- 单点登录

用户登录到运维安全管理系统后，直接选择目标资产及从账号，由运维安全管理系统完成账号及密码的代填，实现自动登录。

- 自动捕获用户命令行输入，智能识别命令和编辑输入

核心服务层可以自动捕获用户命令行输入，如 ls，ps，ifconfig 等。

核心服务层支持多行长命令的捕获，多行命令的编辑操作（如回退，DEL，光标移位等）不影响命令捕获结果。核心服务层智能地支持历史操作，支持 UP，DOWN 功能键，支持对历史操作命令的抓取，支持对以“！”方式执行历史命令的控制和相关命令抓取。核心服务层智能识别编辑状态和命令状态，支持对所有 shell 下命令的抓取，支持 mysql，telnet，ssh 等客户端程序内部呈现命令的捕获功能。

- 支持 TAB 补齐等 Readline 功能

核心服务层支持命令的 TAB 补全，支持回退键、删除键、方向键等功能键。

- 支持组合命令的动作审计

核心服务层支持命令的组合使用，支持管道“|”，支持逻辑或“||”和与“&&”操作，支持分号命令“;”。核心服务层支持拒绝和允许两个策略动作。对拒绝的命令，核心服务层能够保证该命令不被执行，忠实地履行安全策略执行动作。

5 产品功能与特性

5.1 产品功能

运维和审计管理平台，将运维人员离散维护主机及网络设备的行为统一到该平台进行，加强对系统安全以及运维的控制力。一方面通过集中运维，减少因离散操作导致的失误，提高工作效率，如新的安全策略在主机上的统一应用等；另一方面通过对所有用户在主机上的操作行为进行监控与记录，实时了解用户的操作行为，发现风险及时中止用户的操作，并记录下用户所有的操作行为，便于进行事后的审查与取证。

5.1.1 账号管理

帐号管理包含对所有服务器、网络设备帐号以及所有使用运维安全管理系统自然人的账号实行集中管理。账号的集中管理是集中授权、认证和审计的基础。集中帐号管理可以完成对帐号整个生命周期的监控和管理，而且降低了设备管理

员管理大量用户帐号的难度和工作量。同时，通过统一的管理还能够发现帐号中存在的安全隐患，并且制定统一的、标准的用户帐号安全策略。

通过建立集中帐号管理，可实现帐号与实际自然人相关联。通过这种关联，可实现多级的用户管理和细粒度的用户授权。而且，还可以实现针对自然人的实名行为审计，真正满足审计的需要。

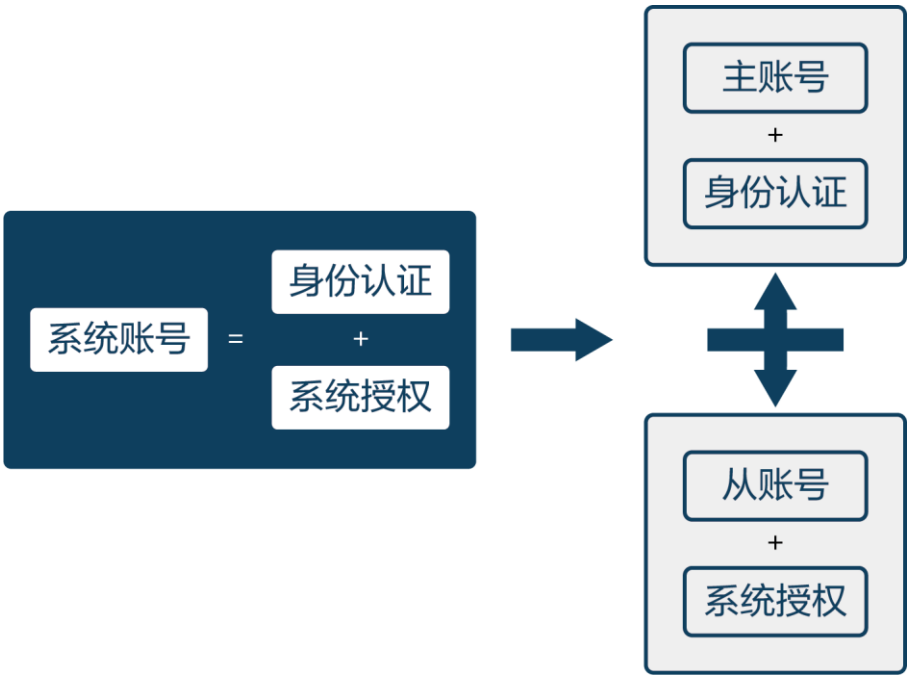

图 5.1 集中账号管理

- **主账号管理**

使用运维安全管理系统的用户与真实人员是唯一对应的，普通用户即为主账号。主账号管理将实现对用户的集中管理及用户的集中授权管理。主账号管理功能包括主账号的创建、主账号基本信息维护、主账号资源角色授权（主账号资源访问授权）、主账号的锁定、主账号删除等。除此之外，还可以通过角色划分功能，区分人员类别，比如一线、二线岗位、不同中心员工或外包人员等。

- **从账号管理**

资源管理与主账号管理同样是系统的核心部分。资源管理主要负责管理不同类型的资源，其中包括不同类型主机系统、网络设备、安全设备等。这些不同类型的资源组成了整个运维安全管理系统的访问对象，也是保护对象。

资源管理主要包含两个大模块：资源管理和资源从账号管理。资源管理主要是对不同类型的资源进行划分。从账号管理则依附于不同的资源。访问资源就是访问资源的从账号，这里也是管理员操作和运维人员操作的核心部分。

- **从账号口令变更**

依照等级保护和分级保护的基本要求，对于内网设备的口令需要定时按照一定的复杂程度进行变更，运维安全管理系统提供自动定时批量修改从账号口令的功能。用户可自定义口令变更时间、周期、复杂程度等内容。极大地减轻了运维人员的工作压力。

5.1.2 授权管理

深信服运维安全管理系统通过灵活的授权管理和细粒度的访问控制管理可以对用户对各种资源的访问进行控制和审计。

- **灵活的授权管理**

深信服运维安全管理系统提供统一的界面，对用户、角色与行为、资源进行关联授权，以达到对权限的细粒度分配，最大限度保护 IT 资源的安全。

在集中授权里强调的“集中”是逻辑上的集中，而不是物理上的集中。即在各网络设备、主机系统、安全设备中可能还拥有各自的权限管理功能，管理员也由各自的归口管理部门委派，但是这些管理员从统一的授权系统进去以后，可以对各自的管理对象进行授权，而不需要进入每一个被管理对象才能授权。

- **细粒度的访问控制管理**

深信服运维安全管理系统能够提供细粒度的访问控制管理。细粒度的命令策略是命令的集合，提供基于黑白名单的命令清单配置，该命令策略可分配给运维自然人或后台设备，另外也可提供基于访问时间、访问地点、资源、系统帐号、操作命令、自定义命令的强访问控制。通过对访问内容的监控和记录、对危险命令的过滤，实现内部访问的安全运作。

访问控制策略是保护系统安全性的重要环节，制定良好的访问控制策略能够有效提高系统的安全性。

5.1.3 认证管理

- **认证方式多样性**

深信服运维安全管理系统为用户提供统一的认证接口。采用统一的认证接口不但便于对用户认证的管理，而且能够采用更加安全的认证模式，提高认证的安全性和可靠性。

深信服运维安全管理系统自身是经过加固的可防御进攻的安全设备，支持静态口令、动态口令、 USB-KEY、数字证书、动态令牌、生物特征等多种组合认证方式，并且传输过程加密。

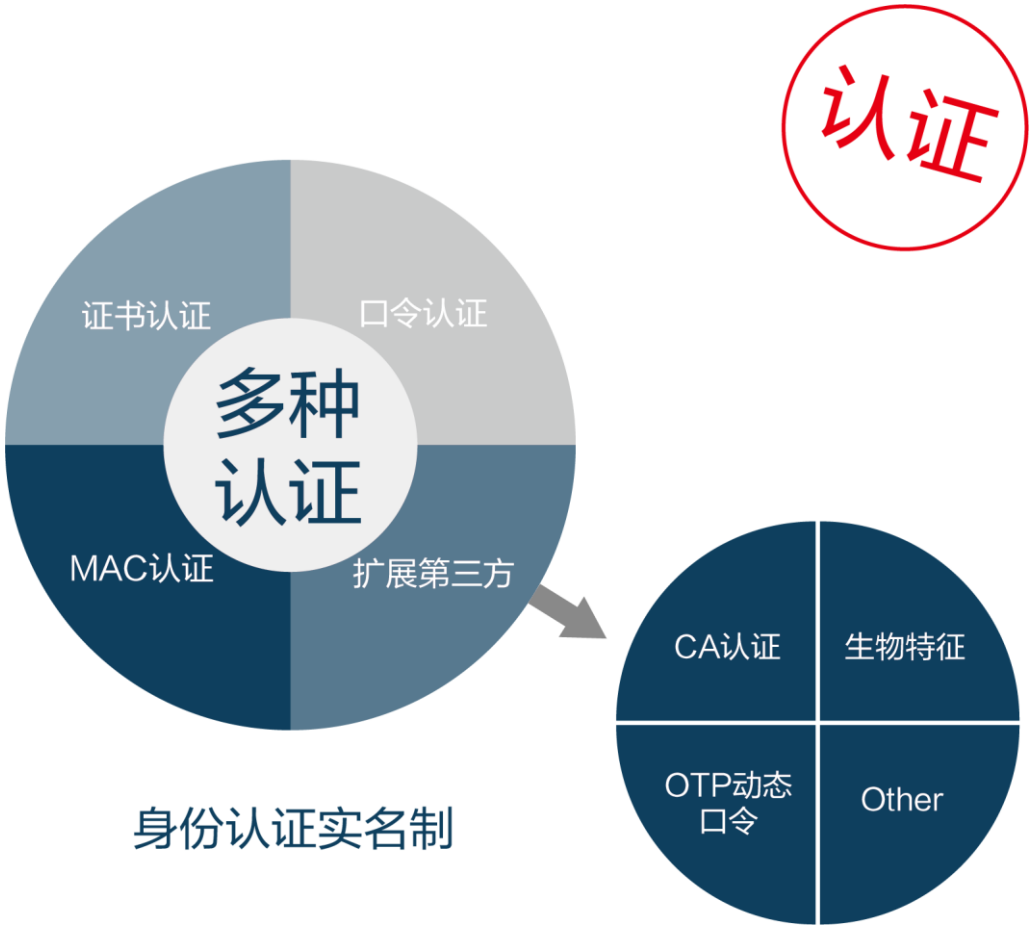

图 5.2 认证方式

- **单点登录（SS0）**

深信服运维安全管理系统提供了基于 B/S 的单点登录，在整个 IT 系统中具有多帐号的用户提供了方便快捷的访问途径，运维人员通过一次登录运维安全管理系统，就可以访问被授权的多个设备资源，无需再次手动输入设备账号和密码信息，而且访问不同系统不用重复登录，提高了运维的效率，改善用户体验。同时，集中的单点登录便于全系统采用强认证，从而提高了用户认证环节的安全性。

深信服运维安全管理系统基于人性化设计，直接通过 WEB 方式实现单点登陆，方便运维人员操作，简化前端运维环境。

5.1.4 访问控制

- **实时监控与阻断**

深信服运维安全管理系统能够实现对运维人员在线操作的实时监控功能，审计员可以以图像方式实时地监视运维人员的运维操作，如果发现运维人员存在不合规的操作，审计员有权限实现对当前会话的实时阻断。

- 访问控制策略

深信服运维安全管理系统能够制定基于黑白名单的访问控制策略，用以限制用户访问目标设备的访问命令，该策略支持正则表达式。

5.1.5 审计管理

- **详尽的操作审计**

深信服运维安全管理系统提供详尽的操作审计功能，主要审计操作人员的帐号使用（登录、资源访问）情况、资源使用情况等。在各服务器主机、网络设备的访问日志记录都采用统一的帐号、资源进行标识后，操作审计能更好地对帐号的完整使用过程进行追踪审计。由于运维安全管理系统采用单点登录（SSO）方式，自然人与堡垒账号实现一一对应，审计员可以轻松的将系统操作与自然人相对应，解决了以往运维环境中仅追查到设备账号层面的问题，方便了安全事故的定责工作。

深信服运维安全管理系统提供命令审计、内容审计和录像审计。对不同设备、不同访问方式都有详尽的操作审计，真实、直观地重现操作人员的操作过程。系统支持操作协议：Telnet、FTP、SFTP、SSH、SSH2、RDP、X windows、VNC 等。

深信服运维安全管理系统通过系统自身的用户认证系统、用户授权系统，以及访问控制等详细记录整个会话过程中用户的全部行为，还可以将审计日志传送给第三方。

- **完备的审计报表**

深信服运维安全管理系统提供完备的审计报表。运维安全管理系统管理员可以按照用户定义条件，以及系统自定义的报表模板制定综合报表；系统可按照访

问者、被保护对象、行为方式、操作内容等自动生成统计报表，并能按照用户的要求添加、修改报表数量、格式及内容，以满足审计的要求。

- **内部审计**

深信服运维安全管理系统提供完备的内部审计记录，可完整记录运维安全管理系统管理员的管理行为，如主/从账号管理、策略修改、登入、登出等内容。

5.2 产品特性

5.2.1 充分考虑产品自身安全

- **更安全的操作系统及应用**

深信服运维安全管理系统自身采用经过安全加固的操作系统，自身具备操作系统安全配置基线，提升了自身安全性。同时产品本身不停迭代最新操作系统及应用漏洞信息确保产品无可检测出的安全漏洞

- **完善的加密措施**

深信服运维安全管理系统对访问会话代理全程提供通信加密防护，自身业务数据及审计录像文件均密文保存。

5.2.2 多样化的访问控制管理能力

- **命令过滤及审批**

深信服运维安全管理系统支持对关键指令执行时设置黑名单功能，自动阻断违规或高位操作的指令。

同时支持通过命令审批的方式对资源进行保护。即当在控制名单内的命令被请求执行时，需要进行审批，审批通过后，该命令才可以被执行，否则命令请求将被阻断。

- **多级流程审批**

关键资源被访问时需要预定义的审批链中的审批人逐级审批通过后才能访问资源，逐级审批可以定义通过投票数，只有达到最低通过投票数要求，才能算本级审批通过。

- **交叉授权能力**

访问关键设备时需要双人操作，在双方都同意时才能访问关键设备，通过定义双人授权审批人和被审批人来实现双人操作，双人授权是一组相互关联的访问审批关系，可以定义多个审批人和被审批人，如果一个用户既是审批人又是被审批人，根据权限最小化原则，此人在访问设备时以被审批人的身份登陆，需要此授权中的其他审批人审批。

- **组授权能力**

资源组由部门管理员创建，隶属于创建资源组的部门，是部门内资源的集合，同资源可以存在于同一部门下的多个资源组中，便于进行基于资源组的访问授权。实现了用户/用户组对资源、用户/用户组对资源指定账号、用户/用户组对资源组的灵活的访问授权方式。

5.2.3 更加便捷的易用性

- **前端高可用配置**

深信服运维安全管理系统提供前端配置主/备模式双机热备部署功能，主备机切换时长小于 3 秒。

- **支持从用户方 AD 域同步运维用户信息**

支持将 Windows AD 域账号信息周期或一次性同步抽取至本系统，更新深信服运维安全管理系统主账号信息。

- **可灵活自定义的应用运维接入手段**

对于市面上主流的堡垒设备，均可支持对 B/S 系统的单点登录支持。支持手段包括配置表格字段及提交方法，而对于 C/S 系统的单点登录功能则需要研发人员介入编写相应代码。深信服运维安全管理系统可通过配置“动作流”功能完美支持所有 C/S 系统的单点登录功能，用户仅通过在堡垒机前端页面配置“动作流”即可。

5.2.4 更强的用户生产环境适应性

- **支持云端快速部署**

深信服运维安全管理系统支持云端快速部署，实现远程运维管理的规范化；可按照运维人员数量，调整云端服务器配置，即可实现性能优化。

- **客户端高兼容**

深信服运维安全管理系统可完美适配 Windows、linux、国产麒麟系统、Android、IOS、Mac OS 等客户端。

- **全面国产化的支持**

深信服运维安全管理系统可提供全面国产化的解决方案，全面国产化指堡垒机本身的硬件软件国产化、客户的资产、用户的运维客户端三方面的全面国产化。

- **自由选择 Web 方式或运维客户端运维**

深信服运维安全管理系统基于最新的 HTML5 前端技术开发，可实现 web 页面直接运维目标设备，无需安装任何控件，方便快捷。考虑到不改变运维人员运维习惯的需要，深信服运维安全管理系统同时支持调用 SecureCRT、Xshell、Putty、WinSCP、FileZilla、RDP 等客户端工具实现单点登陆。

- **全面支持 IPV6**

深信服运维安全管理系统现已全面支持 IPv6，全面完成向下一代的互联网的平滑演进升级。

6 产品优势与价值

6.1 产品优势

6.1.1 应用接入动作流

用户通过客户端配置可以自定义数据库、C/S、B/S 客户端的属性配置，形成有序的动作流，从而对资源进行运维操作。

通过该功能为用户提供了广泛的应用接入支持，无论被接入（需要单点登录及行为审计）的资源如何设计登录动作，通过动作流都可以简单配置。

6.1.2 强大的口令修改驱动

支持定期或手动变更目标设备真实口令，支持自定义口令变更周期和口令强度。口令变更方式至少支持手动指定固定口令、通过密码表生成口令、依照设备挂载的口令策略生成随机口令、依照密码策略生成同一口令等方式。

改密驱动类型支持 windows 系统、网络设备、linux/unix 系统、数据库等设备。

更为广泛的账号改密驱动，使得深信服运维安全管理系统在用户被管理运维资产类型丰富复杂时有更强的适应性。

6.1.3 角色权限自定义

深信服运维安全管理系统极大程度灵活化系统角色的定义过程，不同于普通的预设固定管理角色权限的堡垒机（如：系统管理员是否能够下载设备口令加密包，配置管理员是否可以修改网络配置），深信服运维安全管理系统可根据实际用户实际的自身管理特性或特殊的安全管理组织架构，划分堡垒机管理角色的管理范畴。

6.1.4 IPV6 全面支持

深信服运维安全管理系统自身网络配置以及被管资源的网络配置均已全面支持 IPV6 并经过市场验证。

6.1.5 多级流程审批

支持自定义多级审批流程，可设置一级或多级审批人，每级审批流程可以指定通过投票数，用户访问关键设备需相关审批人逐级审批通过才允许访问。

6.2 产品价值

6.2.1 实现集中帐号管理，降低管理费用

- **实现对用户帐号的统一管理和维护**

在实现集中帐号管理前，每一个新上线应用系统均需要建立一套新的用户帐号管理系统，并且分别由各自的管理员负责维护和管理。这种相对独立的帐号管理系统不仅建设前期投入成本较高，而且后期管理维护成本也会成倍增加。而通过堡垒机的集中帐号管理，可实现对 IT 系统所需的帐号基础信息（包括用户身份信息、机构部门信息、其他公司相关信息，以及生命周期信息等）进行标准化的管理，能够为各 IT 系统提供基础的用户信息源。通过统一用户信息维护入口，保证各系统的用户帐号信息的唯一性和同步更新。

- **解决用户帐号共享问题**

主机、数据库、网络设备中存在大量的共享帐号，当发生安全事故时，难于确定帐号的实际使用者，通过部署深信服运维安全管理系统，可以解决共享帐号问题。

- **解决帐号锁定问题**

用户登录失败五次，应对帐号进行锁定。网络设备、主机、应用系统等大都不支持帐号锁定功能。通过部署深信服运维安全管理系统，可以实现用户帐号锁定、一键删除等功能。

6.2.2 实现集中身份认证和访问控制，避免冒名访问

- **提供集中身份认证服务**

实现用户访问 IT 系统的认证入口集中化和统一化，并实现高强度的认证方式，使整个 IT 系统的登录和认证行为可控制及可管理，从而提升业务连续性和系统安全性。

- **实现用户密码管理，满足相关政策内控管理的要求**

多数企业对主机、网络设备、数据库的访问都是基于“用户名+静态密码”访问，密码长期不更换，密码重复尝试的次数也没有限制，这些都不能满足内控管理的需求。仅通过制度要求用户在密码更换、密码设定等方面满足相关要求，无法在具体执行过程中对用户进行有效监督和检查。深信服运维安全管理系统通过建设集中的认证系统，并结合集中帐号管理的相关功能，实现用户密码管理，密码自动变更，提高系统认证的安全性。

- **实现对用户的统一接入访问控制功能**

部署堡垒机前，维护人员接入 IT 系统进行维护操作具有接入方式多样、接入点分散的特点。而维护人员中很多是代维人员，这些代维人员来自于各集成商或设备供应商，人员参差不齐，流动性大。由于维护人员对系统拥有过大权限，缺乏对其进行访问控制和行为审计的手段，存在极大的安全隐患。深信服运维安全管理系统统一维护人员访问系统和设备的入口，提供访问控制功能，有效地解决运维人员的操作问题，降低相关 IT 系统的安全风险。

6.2.3 实现集中授权管理，简化授权流程，减轻管理压力

- **实现统一的授权管理**

各应用系统分别管理所属的资源，并为本系统的用户分配权限，若没有集中统一的资源授权管理平台，授权管理任务随着用户数量及应用系统数量的增加越来越重，系统的安全性也无法得到充分保证。深信服运维安全管理系统实现统一的授权管理，对所有被管应用系统的授权信息进行标准化的管理，减轻管理员的管理工作，提升系统安全性。

- **授权流程化管理**

通过深信服运维安全管理系统，管理层可容易地对用户权限进行审查，并确保用户的权限中不能有不兼容职责，用户只能拥有与身份相符的权限，授权也有相应的工作流审批。

6.2.4 实现单点登录，规范操作过程，简化操作流程

- **单点登录**

深信服运维安全管理系统提供了基于 B/S 的单点登录系统，用户通过一次登录系统后，就可以无需认证地访问包括被授权的多种基于 B/S 和 C/S 的应用系统。单点登录为具有多帐号的用户提供了方便快捷的访问途经，使用户无需记忆多种登录用户 ID 和口令。它通过向用户和客户提供对其个性化资源的快捷访问来提高生产效率。同时，单点登录可以实现与用户授权管理的无缝连接，这样可以通过对用户、角色、行为和资源的授权，增加对资源的保护，和对用户行为的监控及审计。

- **规范操作流程**

规范操作人员和第三方代维厂商的操作行为。通过深信服运维安全管理系统的部署，所有系统管理人员，第三方系统维护人员，都必须通过深信服运维安全管理系统来实施网络管理和服务器维护。对所有操作行为做到可控制、可审计、可追踪。审计人员定期对维护人员的操作进行审计，以提高维护人员的操作规范性。

深信服运维安全管理系统规范了运维操作的工作流程，将管理员从繁琐的密码管理工作中解放出来，投入到其他工作上，对第三方代维厂商的维护操作也不再需要专门陪同，从而有效提高了运维管理效率。

6.2.5 实现实名运维审计，满足安全规范要求

- **实现集中的日志审计功能**

各应用系统相互独立的日志审计，无法进行综合日志分析，很难通过日志审计发现异常或违规行为。深信服运维安全管理系统提供集中的日志审计，能关联用户的操作行为，对非法登录和非法操作快速发现、分析、定位和响应，为安全审计和追踪提供依据。

- **辅助审查**

通过集中的日志审计，可以收集用户访问网络设备、主机、数据库的操作日志记录，并对日志记录需要定期进行审查，满足内部控制规范中关于日志审计的需求，真正实现关联到自然人的日志审计。

7 产品应用场景

7.1 账号信息代填、批量改密最佳实践应用-花旗银行

7.1.1 背景概述

花旗银行（Citibank）是花旗集团属下的一家零售银行，其主要前身是 1812 年 6 月 16 日成立的纽约城市银行（City Bank of New York）。

花旗集团在全球一百多个国家约为二亿客户提供服务，包括个人、机构、企业和政府部门。提供广泛的金融产品服务从消费银行服务及信贷、企业、投资银行服务、以及经纪、保险和资产管理等，非任何其它金融机构可以比拟。现汇集在花旗集团下的主要有花旗银行、旅行者人寿、养老保险、美邦、Citi-financial、Banamex 和 Primerica。

银行内部运行有大量的网络设备和服务器。随着各项业务的不断发展，银行各类信息系统和用户数量的不断增加，网络规模迅速扩大，信息安全问题愈见突出，原有的手工管理措施已不能满足目前及未来业务发展的要求。因此需要根据网络现状，建设服务器和设备访问安全管理系统，使得系统和安全管理人员可以对信息系统的用户和各种资源进行集中管理、集中权限分配、集中审计，从技术上保证信息系统安全策略的实施。

7.1.2 实际需求

1) 满足信息安全、IT 系统运维管理、企业遵循三个方面的要求，有效提高银行信息网络的安全性，适应业务的快速发展；
2) 满足全行运维安全管理的整体要求，形成统一管理手段，最小化操作风险；
3) 能提供完备的访问策略管理，提供细粒度的访问授权；
4) 系统应提供统一、集中的管理界面完成策略管理、人员管理、服务器管理，提高系统管理人员的工作效率;
5) 提供对运维人员的强身份认证方法、用技术手段保证操作员的身份证明与其本人的统一；

6) 审计系统应该详细记录操作员的操作行为，能达到客观地再现操作活动的情况，备日后统计；

7) 审计系统记录的操作日志应保证不被操作人员本人篡改或删除，且服务器的宕机也不影响行为审计的独立性。

7.1.3 最佳实践效果

1) 堡垒机提供密码代填功能，业务人员访问数据库服务器时，无需使用账号密码，只通过登录堡垒机就可以完成正常的运维操作，避免了运维人员接触服务器的账号密码；

2) 堡垒机提供批量改密服务，管理员通过堡垒机制定改密策略和周期，堡垒机可以智能完成对于目标服务器的密码修改工作，并将改密后的密码通过邮件的方式发送给管理员，有效地降低了人工成本；

3) 提供完善的身份管理和认证，确保可信用户才能进行操作，解决了 IT 系统中普遍存在的交叉运维而无法定位到具体人的问题，满足审计系统追溯到自然人的要求；

4) 提供基于用户、用户地址、协议、设备地址、时间段、会话时长等组合的授权功能，灵活地解决“能对谁操作”的问题；

5) 提供对正在运维的会话的监控和回放，有效实现事中管理与控制；

6) 提供根据用户安全策略定义违规操作的实时告警和阻断功能，解决“能做什么”的问题；

7) 提供常用运维协议 Telnet、FTP、SSH、SFTP、RDP（Windows Terminal）、VNC 等网络会话的完整会话记录，完全满足内容审计中信息百分百不丢失的要求；

8) 提供详尽的会话审计和回放功能，解决“做了什么”的问题；

9) 提供多层面的审计报表功能，为运维安全管理提供有效数据。

7.2 中国移动通信集团上海有限公司

7.2.1 用户简介

上海移动通信有限责任公司是中国移动（香港）有限公司下属全资子公司，主要经营上海地区的数字蜂窝移动电话（号段：134-139，147，150-152，157-159，

178，182-184，187-188）、IP 电话、互联网接入业务及相关的信息服务、技术开发、技术服务等业务。

7.2.2 客户需求分析

上海移动数据中心机房有数百台运行各类业务的服务器，由众多系统管理员负责管理。由于缺乏相应的先进工具和手段，无法保证系统管理员严格按照规范来进行操作，也无法保证系统管理员的操作行为和管理报告一致。另外，由于服务器众多，系统管理员压力太大等因素，人为误操作的可能性时有发生，这会对部门或者企业声誉造成重大影响，并严重影响其经济运行效能。如何提高系统运维管理水平，满足相关标准要求，降低运维成本，提供控制和审计依据，越来越成为移动关心的问题。

这些问题具体总结如下：

1) 服务器和网络设备的帐号管理混乱，存在共用帐号等问题；
2) 服务器硬件厂商、第三方应用服务提供厂商需要定期维护，分配给他们的用户名/密码容易混乱，并且无法知道他们在服务器上做了些什么样的操作。

7.2.3 产品部署

部署方案：在核心服务器区前架设深信服运维安全管理系统，对所有服务器进行统一集中管理，运维人员通过服务器的相关操作进行监控和审计。

部署深信服运维安全管理系统达到的效果：

1) 实现了对主机、服务器、网络设备、安全设备访问的控制和操作审计。系统界面友好，操作简便。安装部署可以分步骤推进，不影响用户的网络拓扑和正常业务，而且运维人员不需要改变现有运维习惯；
2) 可以很好地实现字符远程终端访问方式的控制，能够设置告警和阻断规则，提供管理员有效的访问控制手段；
3) 系统审计资源使用的全过程，提供三种展现方式：内容、命令、播放，方便管理员对审计信息的查看。不管是字符还是图形的审计结果都支持播放方式，播放过程可以随时调整播放速度、任意拖拽播放进度，方便管理员查找和定位关键操作；

4) 产品达到了对资源使用者访问控制和操作审计的目的，大大提高了网络的安全性，有效的控制了网络内可能发生的违规行为。