聚铭安全运维审计系统

产品白皮书

聚铭网络科技有限公司

2024 年 04 月

目录

声明

在本文中如无特别说明，聚铭网络均指南京聚铭网络科技有限公司和北京聚铭信安科技有限公司。

JUMING 聚铭图标为聚铭网络的商标。对于本手册出现的其他公司的商标、产品标识和商品名称，由各自权利人拥有。

除非另有约定，本手册仅作为使用指导，本手册中的所有陈述、信息和建议不构成任何明示或暗示的担保。

本手册内容如发生更改，恕不另行通知。

如需要获取最新手册，请联系聚铭网络技术服务部。

联系信息

北京总部：北京市海淀区丹棱街 18 号创富大厦 9 层

南京总部：南京市雨花台区软件大道 180 号南京大数据产业基地 7 栋 4 层

电　　话：025-52205520/52205570

传　　真：025-52205565

全国服务热线：400-1158-400

网　　址：www.juminfo.com

产品支持：support@juminfo.com

聚铭网络技术服务以及营销网络覆盖全国，并在各地设有办事处和分支机构，为客户提供无微不至的解决方案和高效的服务支持。聚铭专家团队 7x24 小时全天候在线，确保在安全事件发生时提供分钟级应急响应。

1. 网络运维现状

1.1. 概述

我国经济的高速发展为信息化建设带来了源源不断的动力，现阶段，各行各业无不在信息资产方面增加投入，以确保基础网络、业务系统、数据资产和信息安全方面的需要。高效的信息系统提升了企业的管理水平，提高了工作效率，同时也带来了经济效益。但与此同时，如何维护数量众多的信息资产，让它们健康有序运行，正在引起企业信息部门的关注。信息化建设的重点已经由原来的基础建设向深化应用、安全运维方面发生转变。

随着防火墙、入侵防御系统（IPS）等安全产品的广泛使用，网络已经具备了抵抗外部入侵的能力，但堡垒往往是在内部被攻破的。由于设备和服务器众多，账号管理混乱，授权不清、各种越权访问、误操作、滥用、恶意破坏等情况时有发生。据资料统计，在对网络造成严重损害的案例中，有 70%是组织里的内部人员所为。

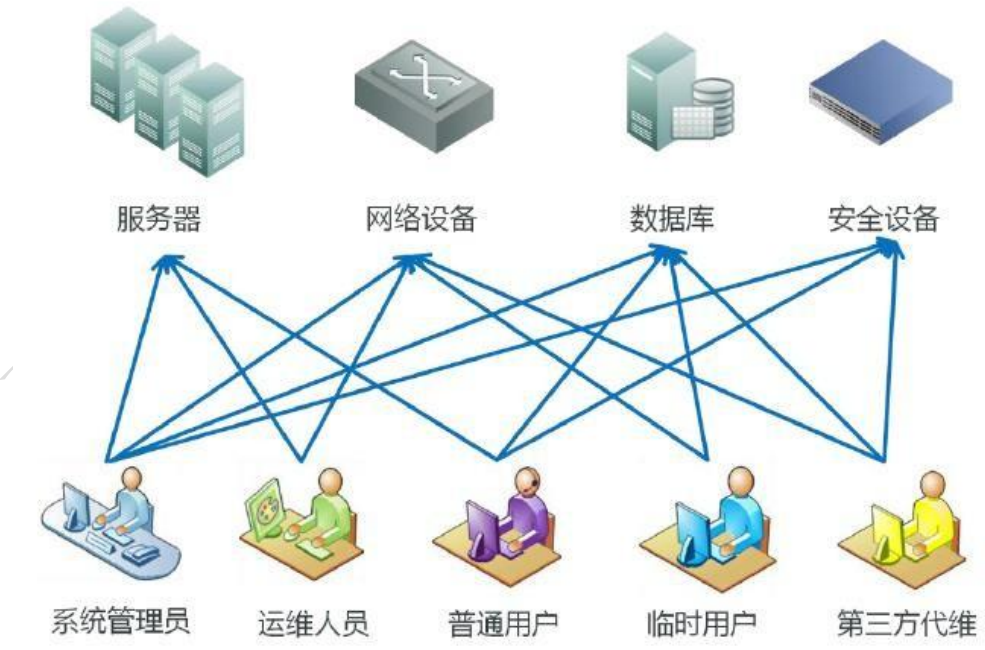
如何提高系统运维管理水平，满足 IT 内控法规遵循的要求，提供控制和审计依据，越来越成为信息部门关心的问题。

1.2.账号共享

为了方便登录，经常出现多人共用账号的情况。多人共享账号在带来方便的同时，导致用户身份的唯一性无法确定。如果其中任何一个人离职或者将账号告诉其他无关人员，会使这个账号的安全无法保证。

由于共享账号是多人共同使用，发生问题后，无法准确定位恶意操作或误操作的责任人。更改密码需要通知到每一个需要使用此账号的人员，带来了密码管理的复杂性。

如下图所示，账号共享或一人使用多个账号会导致整个运维管理过程的复杂混乱。由于整个运维过程的不定因素太多，使得整个运维过程不可控。不仅仅给运维人员带来了巨大的麻烦，而且让管理人员也无法准确的定位责任人，如果长期在这种传统的模式下运维，将会给企业带来巨大的损失，甚至还无法追究责任。所以我们要建立新的运维模式和运维理念。



共享帐户

1.3. 授权不清

在传统的运维模式中，授权是不清晰的，例如:运维人员登录某台服务器或者某个核心交换机等关键设备的时候，他将拥有很大的权限，同时他也可以做一些越权的操作，比如是重启或是其他的敏感操作。也许他的操作是无意的，但都将引发不可估量或者无法挽回的后果。

1.4. 缺乏审计

在传统运维模式下，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。每个网络设备，每个主机系统分别进行审计，安全事故发生后需要排查各系统的日志，但是往往日志找到了，也不能最终定位到行为人。

1.5. 代维人员

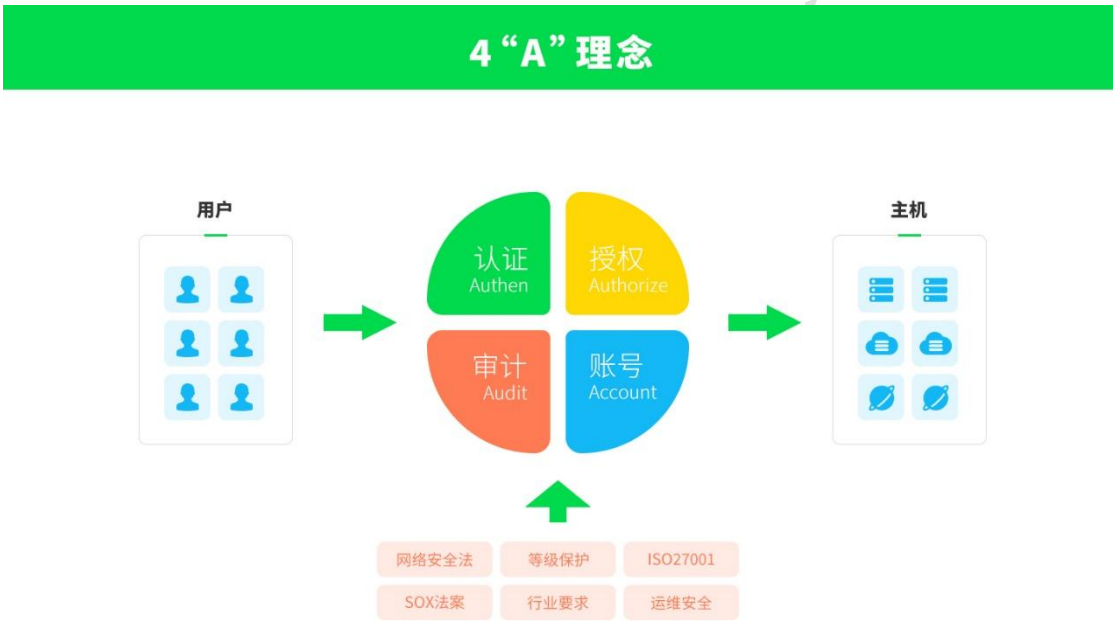
目前，越来越多的企业选择将非核心业务外包给设备商或代维公司，企业在享受便利的同时，同时也带来了更多的问题：代维人员流动性大、缺少操作行为监控、第三方代维人员的权限过大等等，这些问题带来的风险日益凸现。

1.6. 法规遵从

为加强信息系统风险管理，政府、金融、运营商等陆续发布信息系统管理规范和要求，如“信息系统等级保护”、“商业银行信息科技风险管理指引”、“企业内部控制基本规范”等均要求采取信息系统风险内控与审计，但很多企业并没有明确有效的技术手段来达到或满足这些要求。

2. 方案设计

为满足用户对加强内部运维安全日益迫切的需要，聚铭依托自身强大的研发能力，丰富的行业经验，自主研发了新一代软硬件一体化安全运维审计系统——聚铭安全运维审计系统（以下简称”JUMING-SOA”）。该产品支持对企业运维人员在运维过程中进行统一身份认证、统一授权、统一审计、统一监控，消除了传统运维过程中的盲区，实现了运维简单化、操作可控化、过程可视化，是企业 IT 内控最有效的管理平台。



2.1. 设计目的

JUMING-SOA 通过逻辑上将人和目标设备分离，建立“人→主账号（JUMING-SOA 用户账号）→授权→从账号（目标设备账号）→目标设备”的管理模式。在此模式下，通过基于唯一身份标识的集中账号与访问控制策略，与各服务器、网络设备等无缝连接，实现集中精细化运维操作管控与审计。

2.2. 设计理念

管理解决的是面的问题，技术解决的是点的问题，管理的模式决定了管理的高度。我们认为随着应用的发展，设备越来越多，维护人员也越来越多，我们必须由分散的管理模式逐步转变为集中的管理模式。

只有集中才能够实现统一管理，也只有集中才能把复杂问题简单化，集中管理是运维管理思想发展的必然趋势，也是唯一的选择。集中管理包括：

■ 集中账号管理

基于唯一身份标识的全局管理，实现了单点登录，任何运维人员都无法绕过 JUMING-SOA。统一账号管理策略，实现与各服务器、网络设备等无缝连接。

■ 集中授权管理

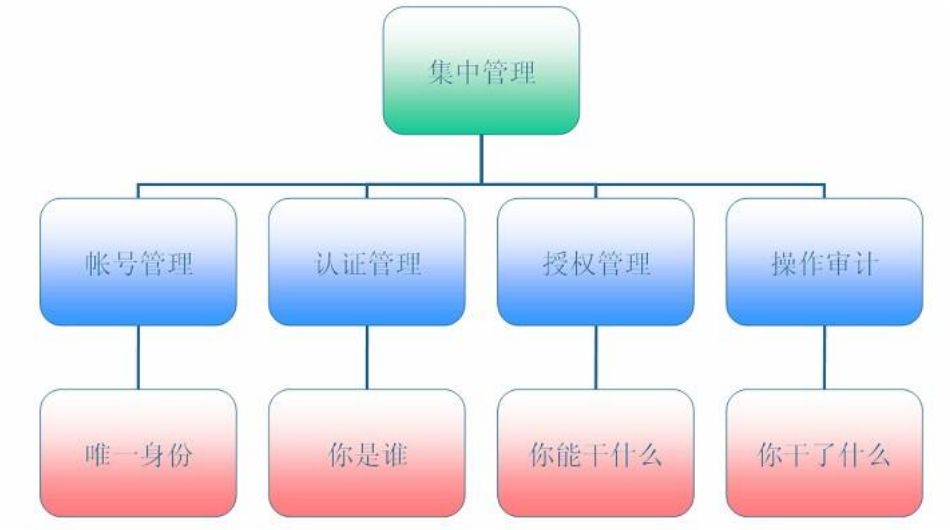
细粒度的命令级授权策略，针对运维人员、服务器、服务器账号、服务器应用、访问时间等多个因素设定细粒度的授权策略，使得运维人员的权限得到很细的划分，从而杜绝了运维人员权限不明晰的问题。

■ 集中认证管理

JUMING-SOA 提供了多种认证方式，包括：本地认证、证书认证、RADIUS 认证及生物指纹识别认证。集中认证有效地将非法用户或非授权用户拒之门外，就像一座堡垒坚不可破。

■ 集中操作审计

基于唯一身份标识，全程审计用户对从登录到退出的操作行为，使得事后的审计和责任的定位有了可靠有力的根据。



2.3. 系统架构

JUMING-SOA 由功能管理模块、平台管理模块和平台接口构成。总体架构如下图所示：

安全运维审计系统系统架构图

2.4.解决方案

JUMING-SOA 通过“物理旁路，逻辑串联”的方式完成部署（也可以采用直通模式），建立集中的运维操作监控平台，建立基于唯一身份标识的实名制管理，统一账号管理策略。通过集中访问控制与授权，实现单点登录（SSO）和细粒度的命令集访问授权。基于用户的审计将直接审计到人，实现从登录到退出的全过程操作行为审计，满足合规管理和审计要求。

2.4.1 管控对象

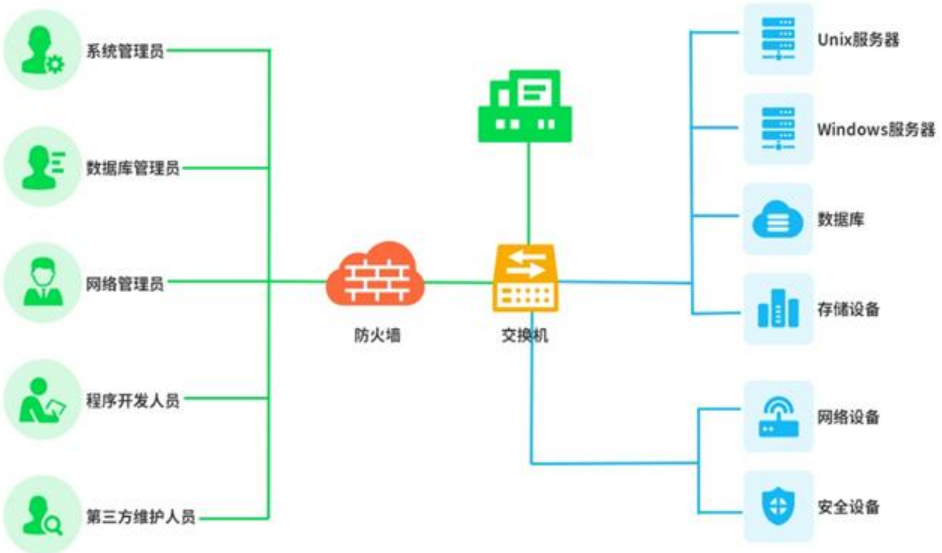
用户	管理人员、运维人员、代维人员（第三方）
资产	服务器（Unix/Linux/Windows）、网络设备、安全设备、数据库

2.4.2 支持协议类型

字符型协议	SSH、Telnet、Rlogin
图形协议	RDP（6.x/7.x/8.x）、VNC
数据库协议	Oracle（8i/9i/10g/11g）、Sybase、MySQL、SQLServer、DB2……
文件传输协议	FTP、SFTP、SCP
其他协议	http、https

2.4.3 部署方式

将 JUMING-SOA 连接到交换机，保证其 IP 可达。通过配置交换机或被管理设备的访问控制策略，仅使 JUMING-SOA 的 IP 可以访问需要管理的设备。



产品部署逻辑图

2.4.4 系统管理员运维过程

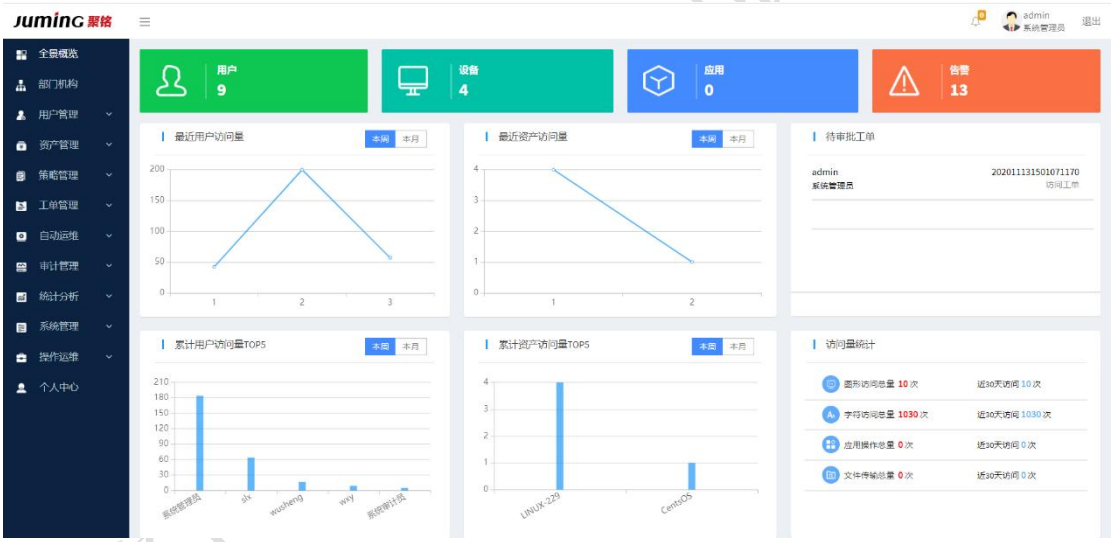
① 添加设备

② 添加从账号

③ 添加主账号

④ 建立主账号到设备的访问控制和审计策略

⑤ 对管理员配置过程全过程审计



2.4.5 运维人员运维过程

① 登录请求

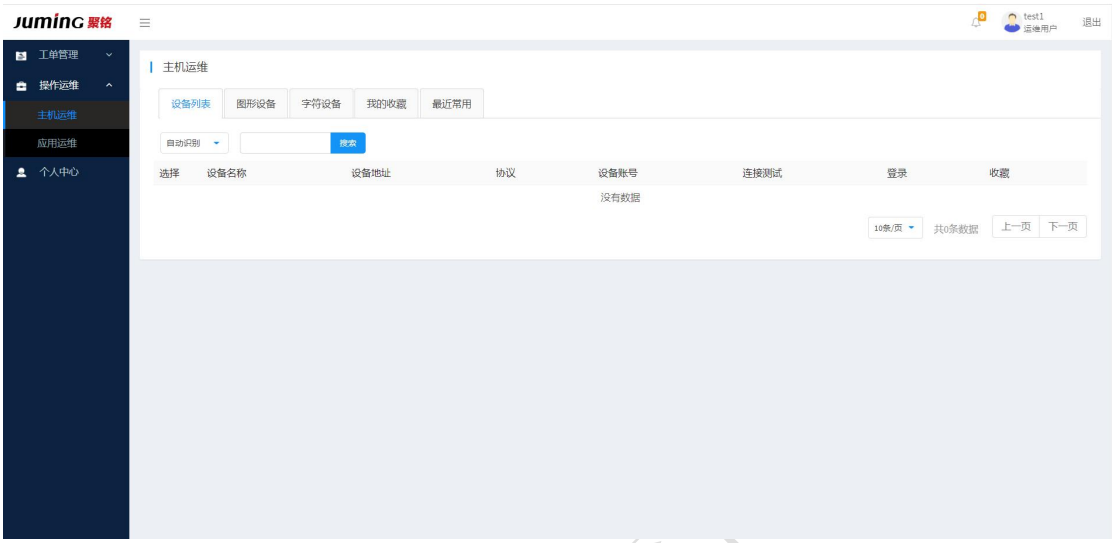
② 登录认证

③ 检查主账号访问权限

④ 访问目标设备

⑤ 返回访问结果

⑥ 访问过程审计



3. 主要功能介绍

3.1. 单点登录

JUMING-SOA 提供了基于 B/S 的单点登录系统，运维人员通过一次登录系统后，就可直接对多种基于 B/S 和 C/S 的应用系统，而无需再次认证过程。单点登录为具有多账号的用户提供了方便快捷的访问途径，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提高了工作效率。同时，系统自身是采用强认证（动态口令及生物识别指纹认证）的系统，从而提高了用户认证环节的安全性。单点登录可以实现与用户授权管理的无缝连接，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。

3.2. 集中账号管理

集中账号管理包含对所有服务器、网络设备账号的集中管理。账号和资源的集中管理是集中授权、认证和审计的基础。集中账号管理可以完成对账号整个生命周期的监控和管理，而且还降低了管理大量用户账号的难度和工

作量。同时，通过统一的管理还能够发现账号中存在的安全隐患，并且制定统一的、标准的用户账号安全策略。

通过建立集中账号管理，企业可以实现将账号与具体的自然人相关联。通过这种关联，可以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行为审计，以满足审计的需要。

3.3. 身份认证

JUMING-SOA 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。集中身份认证提供静态密码、动态口令和生物识别指纹认证方式等多种认证方式，其中指纹认证模块以活体生物指纹特征识别技术为核心，大大增强安全运维审计系统用户认证的唯一性，而且系统具有灵活的定制接口，可以方便的与第三方认证服务器对接。

3.4. 资源授权

JUMING-SOA 提供统一的界面，对用户、角色及行为和资源进行授权，以达到对权限的细粒度控制，最大限度保护用户资源的安全。通过集中访问授权和访问控制可以对用户通过 B/S、C/S 对服务器主机、网络设备的访问进行审计和阻断。在集中访问授权里强调的“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、服务器主机系统中可能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，但是这些管理员在 JUMING-SOA 上，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。授权的对象包括用户、用户角色、资源和用户行为。系统不但能够授权用户可以通过什么角色访问资源这样基于应用边界的粗粒度授权，对某些应用还可以限制用户的操作，以及在什么时间进行操作等的细粒度授权。

3.5. 访问控制

JUMING-SOA 能够提供细粒度的访问控制，最大限度保护用户资源的安全。

细粒度的命令策略是命令的集合，可以是一组可执行命令，也可以是一组非可执行的命令，该命令集合用来分配给具体的用户，来限制其系统行为，管理员会根据其自身的角色为其指定相应的控制策略来限定用户。

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

3.6. 操作审计

操作审计管理主要审计操作人员的账号使用（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账号、资源进行标识后，操作审计能更好地对账号的完整使用过程进行追踪。

内控堡垒主机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日志。还可以将产生的日志传送给第三方。

4. 关键技术应用

4.1. 逻辑命名自动识别技术

JUMING-SOA 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新的突破，可以更加准确的控制用户意图。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。

4.2.分布式处理技术

JUMING-SOA 采用分布式处理架构进行处理，启用命令捕获引擎机制，通过策略服务器完成策略审计，通过日志服务器存储操作审计日志，并通过实时监视中心，实时察看用户在服务器上的行为。这种分布式设计有利于策略的正确执行和操作记录日志的安全。同时，各组件之间采用安全连接进行通信，防止策略和日志被篡改。各组件可以独立工作，也可以分布于不同的服务器上，亦可将所有组件安装于一台服务器上。

4.3.图形协议代理

为了对图形终端操作行为进行审计和监控，JUMING-SOA 主机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 XWindow 方式图形终端操作。

4.4.数据加密技术

JUMING-SOA 在处理用户数据时采用国密 SM4 进行数据加密技术来保护用户通信的安全性和数据的完整性，并支持硬件加密卡进行硬件加密，防止恶意用户截获和篡改数据，充分保护用户在操作过程中不被恶意破坏。

4.5.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。JUMING-SOA 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。

4.6.动态口令技术

安全运维审计系统往往具有 SSO 功能，这意味着只要取得了用户安全运维审计系统主账号，就可以登录到这个用户拥有权限的所有主机，因此，安全运维审计系统往往会成为一个安全的薄弱点。

与其它厂商运维审计产品不同，JUMING-SOA 系统内置了动态口令产品，而其它厂商都需要购买第三方厂商的动态口令产品才能实现对主账号的密码保护，相比之下，JUMING-SOA 具有内置的动态口令系统可以有效的降低用户采购和管理成本，在一个系统中对所有用户和令牌进行管理，而不需要分别在一套系统中管理用户，另一套系统中管理用户和令牌。

4.7.指纹认证技术

聚铭安全运维审计系统生物识别指纹认证模块采用国际领先的指纹特征识别算法、基于活体识别技术自主开发的具有自主知识产权的生物识别指纹身份认证系统。

系统以活体生物指纹特征识别技术为核心；采用模块系统结构，保证系统具有高性能、高可靠性、高扩展性；遵循国家信息安全标准，对用户信息采取加密传输和存储措施，保证用户信息的安全。为应用系统提供多种安全应用模式和不同封装层次的安全开发接口。为安全运维审计系统用户认证唯一性提供强有力的技术手段。

5.产品优势

5.1.强大的应用发布系统

用户通过应用发布系统，能够极为方便的将用户需要管理系统托管至 JUMING-SOA 系统，包括但不限于用户自主开发的各类应用及各类数据库应用。

严格限制运维用户的访问权限，对于仅需要对某些应用进行运维操作的用户，使用应用发布系统，使其仅能访问需要运维的应用，而无法取得远程操作系统的管理权限。

应用发布系统允许使用单应用模式，也可以使用多应用模式，多应用模式可以在多个应用之间进行复制粘贴，此外应用发布系统可以按需关闭某些应用中的图形界面功能。

5.2. 审计信息“零管理”

JUMING-SOA 支持“日志零管理”技术，所有管理员需要日常进行的操作日志均可由系统定时自动后台运行。

日志自动维护：根据日志自动维护计划的设置，系统在指定时间自动进行相应的日志数据备份。

日志查询：系统提供多种审计日志查询条件，包括时间、IP 地址、用户名、设备名、关键字、危险等级（高、中、低）等；

审计报表：系统提供详细的多种类别的报表模板，可提供基于操作时长、高危操作、阻断操作等类别的用户操作 TOP10。系统支持生成：日、周、月、年度综合报表，报表支持 MSWord、Html 等格式导出，降低维护费用与管理员的工作强度。

5.3. 强大丰富的管理能力

支持 B/S 管理方式，Web 管理灵活方便，适合在任何 IP 可达地点远程管理。JUMING-SOA 提供带外管理功能，解决远程应急管理的需求，减少用户运营成本、提高运营效率、减少宕机时间、提高服务质量。

5.4.方便灵活的可扩展性

JUMING-SOA 支持多个硬件管理口，管理口即插即用，提供对多个区域网段的同时管理能力；JUMING-SOA 支持通过发送邮件、日志数据库记录、打印机输出、运行自定义命令等响应方式及时报警。

5.5.高可靠的自身安全性

JUMING-SOA 采用专门设计安全、可靠、高效的硬件运行平台。硬件平台采用严格的设计和工艺标准，保证高可靠性；独特的硬件体系结构大大提升处理能力；操作系统经过优化和安全性处理，保证系统的安全性；

JUMING-SOA 具有更强的高可用性，设备支持热插拔的冗余双电源，避免电源硬件故障时设备宕机，提高设备可靠性；

JUMING-SOA 通信采用强加密的 SSL/TLS 传输控制命令，完全避免可能存在的嗅探行为，确保数据传输安全。

6.结语

企业内部网络安全存在诸多的问题，每种问题都不可小视，对于这些问题，企业内部应该规范管理，应该使用更为先进的 IT 技术手段、技术工具来帮助管理员进行规范化管理，这样才能够保证企业内部网络的安全性。内控堡垒主机使得企业内部网络的管理合理化、安全化、专业化和规范化，充分保障企业网络资源和信息资源的安全。