聚铭安全运维审计系统
产品白皮书

南京聚铭网络科技有限公司

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。

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

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. 需求背景

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。

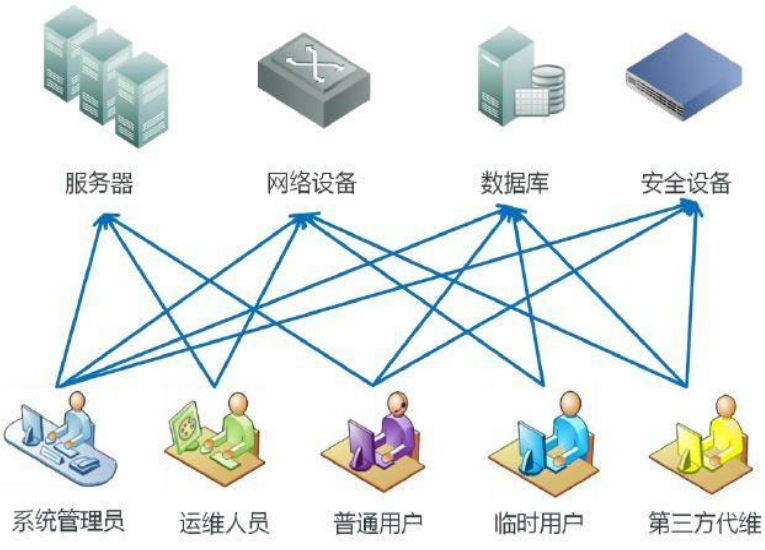
1.2 网络运维现状

1.2.1 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

1.2.2 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。

1.2.3 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。

1.2.4 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。

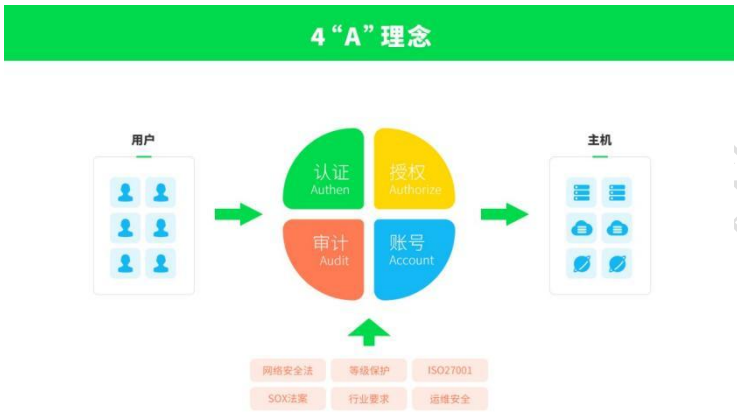
1.3 政策法规要求

当前，国内针对运维安全管理的政策合规要求持续收紧：

法规/标准	核心要求
网络安全法	网络运营者须采取技术措施确保网络安全，留存相关网络日志
等保 2.0（GB/T 22239-2019）	三级及以上系统须实施特权账号双因子认证、操作全程留痕、异常行为审计
数据安全法	对重要数据的访问行为须实施全程记录与访问控制
个人信息保护法	涉及个人信息的数据库访问须具备完整的审计追溯能力
信息技术应用创新（信创）	核心 IT 基础设施须支持国产化软硬件替代
商用密码法规	政务、金融等重点行业须推广使用国密算法（SM 系列）

2. 产品设计

为满足用户对加强内部运维安全日益迫切的需要，聚铭安全运维审计系统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

安全运维审计系统通过逻辑上将人和目标设备分离，建立“人→主账号（安全运维审计系统用户账号）→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安全运维审计系统。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

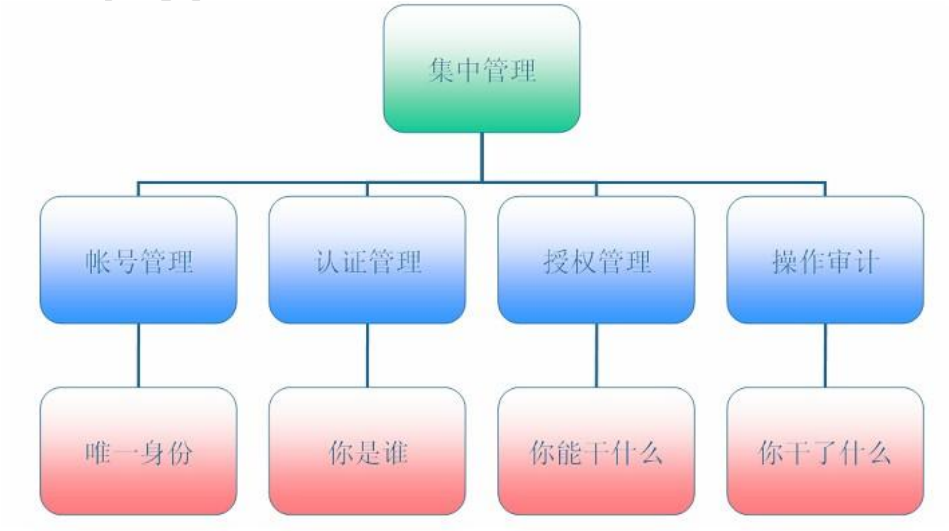
细粒度的命令级授权策略，针对运维人员、服务器、服务器账号、服务器应用、访问时间等多个因素设定细粒度的授权策略，使得运维人员的权限得到很细的划分，从而杜绝了运维人员权限不明晰的问题。

集中认证管理

安全运维审计系统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

聚铭安全运维审计系统由功能管理模块、平台管理模块和平台接口构成。总体架构如下图所示：

聚铭安全运维审计系统系统架构图

2.4 解决方案

聚铭安全运维审计系统通过“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）

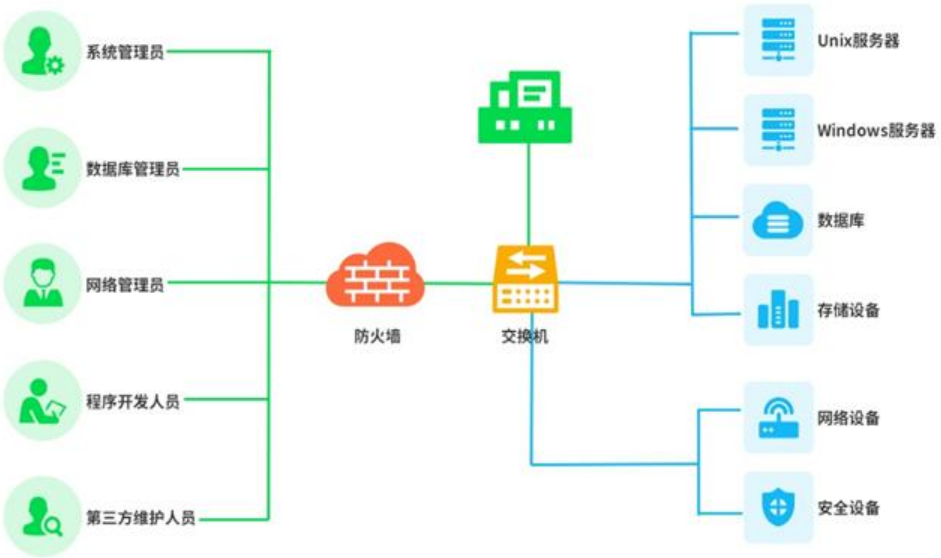
资产	服务器（Unix/Linux/Windows）、网络设备、安全设备、数据库

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

将聚铭安全运维审计系统连接到交换机，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，仅使安全运维审计系统的 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

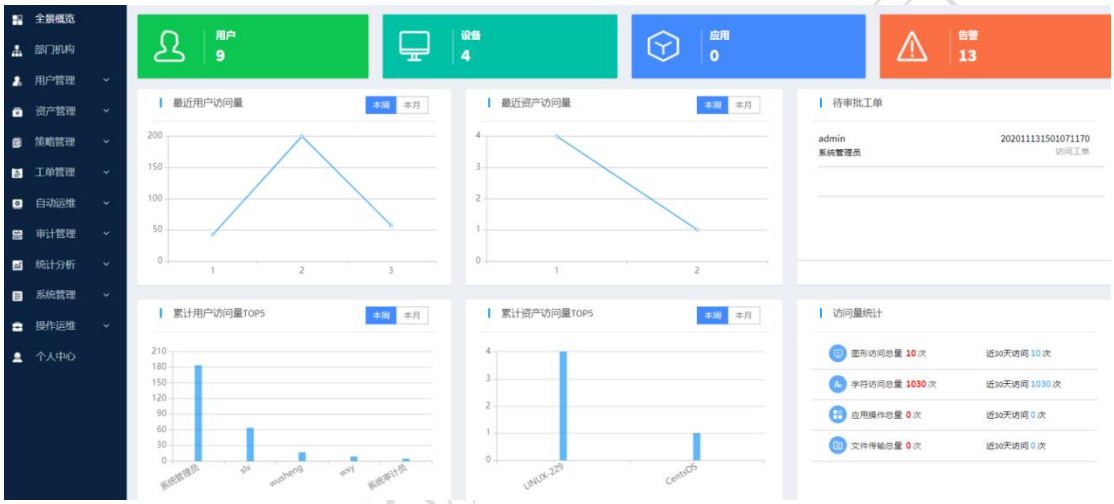
① 添加设备

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

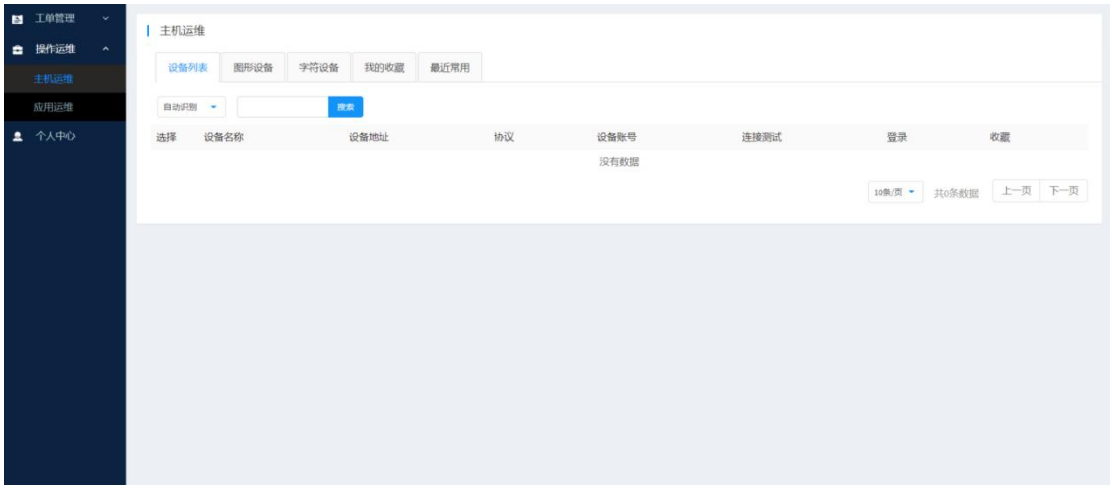
② 登录认证

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. 核心功能体系

3.1 身份治理

3.1.1 多因子认证体系

支持多种认证方式，任意两两组合形成双因子认证，实现知识因子、持有因子、生物因子的完整覆盖：

认证类别	认证方式	技术说明
知识因子	静态密码	支持密码强度策略、周期强制更换、到期提醒、防重复校验
知识因子	手机动态令牌（OTP）	出厂默认支持，基于 TOTP/HOTP 标准，无需配置认证服务器
目录服务	LDAP/AD 域认证	支持多服务器配置、匿名/密码认证、定时同步、未同步用户自动添加
目录服务	RADIUS 认证	支持 CHAP/PAP 协议，兼容标准 Radius 认证服务器
生物因子	指纹识别	支持配置内置/外置指纹认证服务器，可进行认证控制

3.1.2 角色与权限管理

系统采用基于角色的访问控制（RBAC）模型，内置 5 种系统角色：

角色	权限范围
系统管理员	全平台配置管理，用户、资产、策略、系统设置全覆盖
审计管理员	专责审计查询、会话回放、报表导出，不可修改业务配置

部门管理员	仅管理本部门范围内的用户与资产，权限隔离清晰
密码管理员	专责账号密码托管查看与改密策略管理
运维用户	仅可访问被授权范围内的资产，执行具体运维操作

支持在 5 种系统角色基础上自定义角色，按需配置细粒度菜单权限范围，满足组织的差异化权限诉求。

3.1.3 用户访问策略

用户策略支持配置以下访问管控维度，策略可关联用户或用户组：

登录时段限制：精细至 7×24 小时颗粒度的登录时段管控

来源 IP 限制：限定用户仅可从指定 IP 范围发起登录请求

有效期管理：支持配置策略有效期，自动到期失效

3.2 资产管理

3.2.1 多类型资产统一纳管

支持对以下资产类型的统一纳管与全生命周期管理：

资产类型	支持协议/范围
主机设备	SSH、RDP、TELNET、VNC、FTP、SFTP、X11；支持 IPv4/IPv6/域名
应用系统	Windows 和国产 Linux 应用发布（Chrome/Firefox/Navicat/PLSQL/SSMS 等）
数据库	MySQL、SQL Server、Redis、Oracle、PostgreSQL、KingBase

3.2.2 智能资产发现

支持按地址段或单地址、自定义端口范围进行网络资产扫描，扫描任务后台异步执行，结果支持批量编辑与归档，显著降低大规模资产录入的人工成本。

3.2.3 设备账号生命周期管理

支持配合密码管理模块实现账号密码的集中托管与定期自动轮换

账号支持精细配置：协议、端口、登录方式、SSH Key、字符集、访问目录等

3.3 访问控制

3.3.1 多维细粒度运维授权

运维授权策略在"用户-资产"关联的基础上，叠加多个访问管控维度，实现最小权限原则的精确落地：

管控维度	配置项说明
时间管控	访问时段精确至 7×24 小时颗粒度
网络管控	来源 IP 范围白名单
操作管控	RDP 磁盘映射、剪切板（RDP/VNC/X11）、SFTP/FTP 文件操作、ZMODEM、提权登录等细粒度开关
会话水印	H5 会话全程水印，包含用户名、姓名等身份属性信息
二次授权	支持策略级开启二次授权，访问时实时触发强制审批

3.3.2 命令级指令控制

针对字符运维会话（SSH/TELNET）的执行命令实施精细化管控：

支持对指令配置**允许执行/指令申请/指令阻断/会话阻断**四种执行动作

支持正则表达式匹配，适应复杂指令模式识别需求

可关联指令集批量管理，涵盖指令名称、风险描述、执行动作

触发阻断类指令时支持配置告警通知方式

3.3.3 工单授权

标准工单：运维人员申请特定资产的时段性访问权限，管理员审批通过后自动授权

二次授权：敏感操作触发时实时向授权人发起二次确认请求

实时弹窗审批：审批人无需主动刷新，工单提交后立即弹窗提醒，大幅压缩审批等待时间

所有审批操作完整记录于审批日志，全过程可追溯

3.4 运维执行

3.4.1 主机运维

Web H5 无插件运维：运维人员无需在终端安装任何插件，通过标准浏览器即可完成 SSH、TELNET、RDP、VNC、SFTP、X11 等协议运维访问，兼容 Chrome、Firefox 等主流浏览器及国产浏览器。

本地客户端直调：支持一键调用运维人员熟悉的本地客户端工具，不改变操作习惯：

Windows 环境：MSTSC、TigerVNC、SecureCRT、PuTTY、XShell、FileZilla、xftp、WinSCP、FlashFXP 等

特色能力：

密码会同机制：支持 A/B 段双角色分别维护密码，通过工单审批实现密码会同，适用于未纳管资产的安全访问场景

批量登录：可同时登录多台设备，提升批量运维效率

资产快速定位：支持按图形/字符设备、我的收藏、最近常用分类展示，快速锁定目标资产

3.4.2 应用运维

支持通过 Web 方式访问已发布的 B/S、C/S 应用，兼容 Windows 及国产化操作系统（麒麟/统信）浏览器环境。应用登录支持密码自动代填，对特殊登录页面可通过自定义 XPath 方式实现精准代填。

3.4.3 数据库安全运维

采用非应用发布模式实现数据库的透明代理运维，支持 MySQL、SQL Server、Redis、Oracle、PostgreSQL、KingBase 等主流数据库：

运维人员通过访问串使用熟悉的数据库客户端（Navicat、SSMS 等）连接，

操作体验与直连完全一致；

所有 SQL 语句在代理层全程截获记录，无需在数据库端安装任何 Agent；

数据库运维操作在数据库审计模块中完整呈现，支持多维条件检索；

3.4.4 会话协同

支持运维人员发起会话协同并邀请其他人员参与，适用于故障应急处置、技术指导等协作运维场景，全程协同操作完整录制留存。

3.5 安全审计

3.5.1 全链路审计覆盖

审计类型	覆盖范围	审计内容
主机审计	SSH/TELNET/RDP/VNC/FTP/SFTP/X11	命令记录、键盘输入、鼠标动作、窗口标题、文件传输、剪切板、会话录像
应用审计	B/S、C/S 应用发布会话	键盘输入、剪切板记录、会话录像、文件传输
数据库审计	MySQL/SQLServer/Redis/Oracle/PostgreSQL/KingBase	SQL 语句全程记录
管理员审计	系统管理操作	增/删/改等管理操作完整记录
登录审计	所有用户登录行为	登录成功/失败、来源 IP、认证方式等

3.5.2 录像回放能力

支持单个录像文件 ≥10G 的超大体积录像稳定播放，不卡顿、不崩溃

支持回放录像下载，支持大剪切板记录转换为文件下载查看

支持精准帧定位播放，适用于离线取证分析场景

3.5.3 实时会话监控

审计管理员可实时监控所有活动会话，支持：

向运维人员运维窗口实时发送提示信息；

实时锁定/解锁活动会话；

一键终止危险会话；

3.5.4 多维报表与定期推送

提供完整的统计分析与报表能力：

报表类型	核心内容
登录报表	用户登录趋势、访问 Top 10 用户、多维筛选导出
运维报表	会话时长统计、命令执行统计、多维筛选导出
权限报表	资产权限关联关系全量查询、应用权限查询
定期报表	日报/周报/月报自动生成与保存，支持查看和下载历史报表

3.6 密码管理

提供完整的设备账号密码全生命周期管理能力：

密码托管：密码管理员可查看已托管资产的账号密码（明文需授权查看），支持按设备名称、账号、部门等条件搜索。

自动改密：支持配置改密策略（改密周期、改密时间、密码强度要求），关联设备账号后按策略自动触发定期改密，支持手动立即改密。支持编排改密脚本，实现全类型资产的差异化改密配置。

密码备份：改密后密码即时备份至邮件/文件服务器，备份文件加密处理，保障备份安全可追溯。

密码会同机制：支持 A/B 段双角色分段持有密码，两个角色各自维护密码的一半，通过密码会同工单审批完成完整密码的临时拼合访问，有效解决未纳管资产或特殊敏感资产的安全访问控制难题，实现"知密分权"。

4. 关键技术应用

4.1 逻辑命名自动识别技术

安全运维审计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

安全运维审计系统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，安全运维审计系统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

安全运维审计系统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。安全运维审计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。

4.6 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，安全运维审计系统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，安全运维审计系统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

安全运维审计系统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. 安全运维审计系统产品优势

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安全运维审计系统系统，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”

安全运维审计系统支持“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 Word、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。安全运维审计系统提供带外管理功能，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

安全运维审计系统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；安全运维审计系统支持通过发送邮件、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

安全运维审计系统采用专门设计安全、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；

安全运维审计系统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；

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。