



# 绿盟运维安全管理系统

## 产品彩页

【绿盟科技】



©2019 绿盟科技

---

## ■ 版权声明

---

本文中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，除另有特别注明，版权均属绿盟科技所有，受到有关产权及版权法保护。任何个人、机构未经绿盟科技的书面授权许可，不得以任何方式复制或引用本文的任何片断。

---

# 一. 产品简介

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建设，转向以深化应用、提升效益为特征的运行维护阶段，IT 系统运维与安全管理正逐渐走向融合。信息系统的安全运行直接关系企业效益，构建一个强健的 IT 运维安全管理体系对企业信息化的发展至关重要，对运维的安全性提出了更高要求。

绿盟运维安全管理系统 V5.6（简称 OSMS 或堡垒机），是一套先进的运维安全管控与审计解决方案，目标是帮助企业转变传统 IT 安全运维被动响应的模式，建立面向用户的集中、主动的安全管控模式，降低人为风险，满足合规要求，保障企业效益。

绿盟堡垒机产品通过逻辑上将人与目标设备分离，建立“人->主账号(堡垒机用户账号)->授权->从账户（目标设备账号）->目标设备”的管理模式；通过基于唯一身份标识的集中账号与访问控制策略，与各个服务器、网络设备、数据库服务器等建立无缝连接，实现集中精细化运维操作管控和审计。



建立基于唯一身份标识的全局实名制管理

基于最小权限原则，让正确的人做正确的事

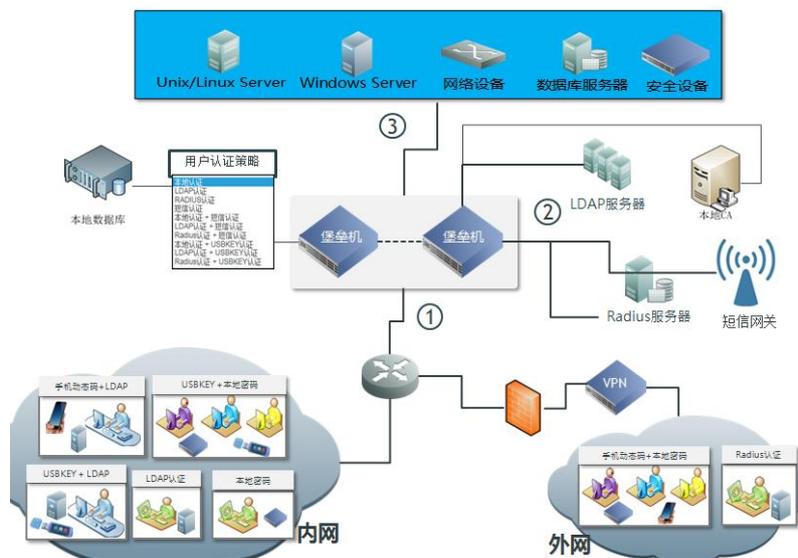
全程操作审计，聚焦关键事件，及时发现，准确可查

## 二. 关键功能

### 2.1 多维度、细粒度的认证与授权体系

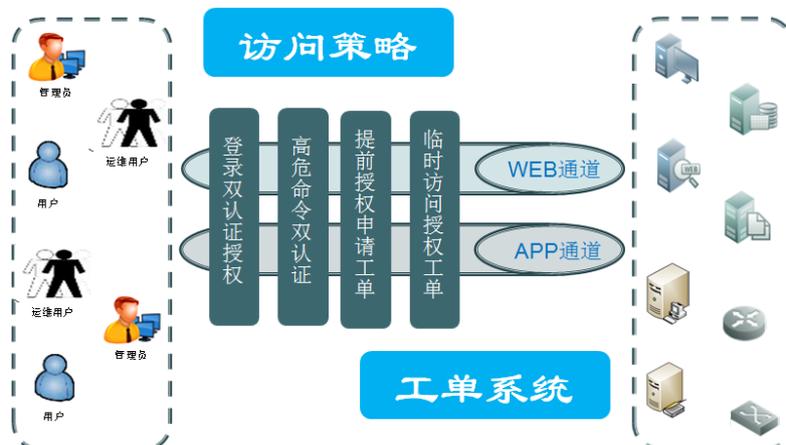
#### ◆ 灵活的认证方式

绿盟堡垒机产品对主账号的认证，支持本地认证、LDAP 认证、RADIUS 认证、USBkey 认证、动态令牌认证等多种方式，能够根据用户实际需求，设置混合认证方式，即不同主账号采取不同的认证方式，实现按需设置认证方式。



#### ◆ 多维度、细粒度的访问控制

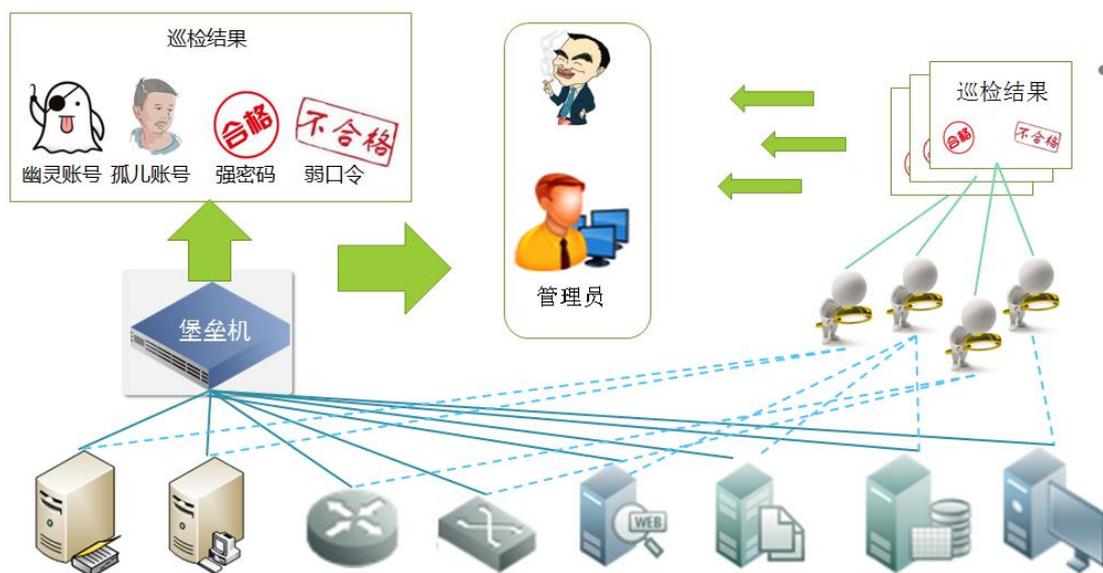
绿盟堡垒机产品支持基于角色的访问控制（RBAC ,Role-Based Access Control）。管理员可按照时间、部门、职责和安全策略等维度，设置细粒度权限策略，让正确的人做正确的事，简化授权管理。



## 2.2 高效率、智能化的资产管理体系

### ◆ 智能化巡检托管设备和设备账号

用户运维环境中常常存在大量的托管设备和设备账号信息，堡垒机能够智能化发现运维人员运维过程违规新建的设备账号(简称幽灵账号)，幽灵账号常常会是系统的后门账号。同时由于运维人员离职，或职责切换等原因，出现已托管的设备账号长期不会被使用(简称为孤儿账号)，因而导致托管设备上存在一定量的孤儿账号，长期以往必然会导致用户托管的设备存在严重的安全隐患，有效防范托管设备中设备账号管理漏洞带来的安全风险。



## 2.3 高保真、易理解、快定位的审计效果

### ◆ 基于唯一身份标识的审计

绿盟堡垒机产品主账号是获取目标设备访问权利的唯一账号，支持本地认证、LDAP 认证、RADIUS 认证、USBkey 认证、短信密码等多种认证方式，将主账号与实际用户身份一一对应，确保不同设备、系统间行为审计的一致性，从而准确确定为事故责任人，弥补传统网络安全审计产品无法准确定位用户身份的缺陷。

### ◆ 全程行为审计

绿盟堡垒机可完整审计运维人员通过账号“在什么时间登录什么设备、做什么操作、返回什么结果、什么时间登出”等行为，全面记录“运维人员从登录到退出”的整个过程，帮助管理人员及时发现权限滥用、违规操作，准确定位身份，以便追查取证。

### ◆ 视频和命令操作双层审计

产品支持指令输入和图形操作双审计技术

- 指令输入审计：运维过程中用户输入的键盘指令可以被审计记录

- 图形操作审计：运维过程中用户图形操作可以被审计记录
- 图形内容识别：运维过程中用户图形操作的窗口标题信息可以被审计记录
- 文字搜索定位录像播放：审计用户可以不用从头到尾查看运维录像，通过搜索键盘或窗口标题信息，直接跳转到当时运维的录像记录。节约审计操作成本。



## 2.4 稳定可靠的系统安全性保障

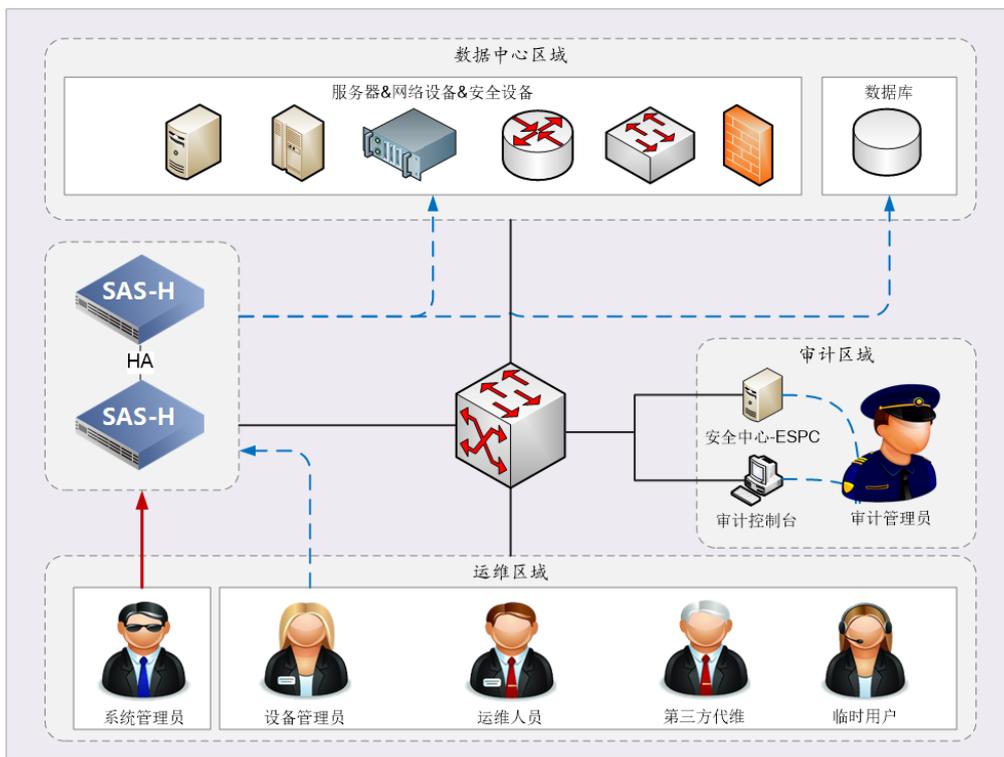
- ◆ 采用专门设计的安全、可靠、高效的硬件平台。该硬件平台采用严格的设计和工艺标准，保证高可靠性；
- ◆ 独特的硬件体系结构提升处理能力；
- ◆ 操作系统经过优化和安全性处理，保证系统的安全性；
- ◆ 支持热插拔的冗余双电源，避免电源硬件故障时设备宕机，具有可靠的高可用性；
- ◆ 堡垒机与客户端通信均采用加密的 SSL 传输控制命令，完全避免可能存在的嗅探行为，确保数据传输安全。
- ◆ 审计日志信息采用专利特有的保存方法，支持关键特殊信息指纹签名，并可加密存储到外置存储设备。仅可在专用审计播放器下查看。
- ◆ 支持智能管理系统存储资源，系统存储达到瓶颈时自动告警或清理存储空间。
- ◆ 支持 RAID1 磁盘阵列实现数据冗余备份，提供高数据安全性和可用性。
- ◆ 用户配置信息采用加密存储，用户配置备份信息仅能通过系统解密获取，防止被不法用户盗取。

## 三. 典型应用

产品主要应用于以下应用场景：

- ✓ 应用场景一 企业运维安全管理，提高运维效率，预防运维风险；
- ✓ 应用场景二 第三方审计机构对运维的审计，满足合规需求；

采用“物理旁路，逻辑串联”部署方式，所有维护人员必须通过堡垒机才可访问目标设备，从而实现对运维人员的操作审计。



## 四. 客户价值

通过部署绿盟堡垒机产品，可帮助企业建立面向用户的集中、有序、主动的运维安全管控平台，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，降低人为安全风险，避免安全损失，满足合规要求，保障企业效益。