



LanSecS<sup>®</sup>

内网安全管理系统

---



## 产品概述

LanSecS<sup>®</sup> 内网安全管理系统通过对计算机入网监测、资产管理、安全加固、运行维护、安全审计、USB移动存储介质等多个方面的综合管理，协助用户打造一个安全、可信、规范、健康的内网办公环境。



## 产品功能

### ● 安全加固

提供补丁集中管理、网络参数集中配置、主机防火墙、主机设备接口、系统安全策略的统一管控，保证终端运行环境的安全可控，保障内网运行的可靠性。

### ● 安全审计

提供针对主机的全方位监控与审计，包括文件操作、文档打印、共享访问、服务与进程活动、系统日志、系统账户等。

### ● 安全运维

通过告警平台、远程协助、软件及文件分发等功能实现远程桌面维护以及安全动态展现、桌面通知、信息发布等。

### ● 资产管理

提供对内网资产和资源的集中管理能力，包括计算机、操作系统、软件、硬件，从而提高资产盘点效率和资产变更预警的及时性。

### ● 网络边界管理

通过入网监测、违规外联功能，对内网网络边界进行安全管控，实时发现非法入网主机并可阻断违规外联行为。

### ● 移动储存介质管理

对移动储存介质进行认证注册管理，实现身份鉴别、授权范围管理、读写权限管理、文件操作动态监控与审计。并根据用户不同使用场景可灵活注册移动储存介质，包括未授权移动存储介质、安全U盘、多分区U盘、专用安全U盘、特权U盘。



## 产品特点

### ● 完善的分级管理架构，“分散不分立”

通过分级管理，系统可实现跨地域分散部署和集中管理。“分散不分立”，形成有效的和有机的内网安全管理架构。

## ● 灵活的分权管理机制，“集中不集权”

系统提供了基于安全角色的授权管理机制，根据功能模块或行政机构的划分自定义安全角色，一种安全角色只能执行其所辖部门范围内的相应安全代理的安全策略和审计事件的管理。“集中不集权”，保证了管理的安全性。

## ● 全方位的安全审计能力，有效地防止信息泄密

系统提供对所有输入/输出设备、文件系统、进程、服务、网络应用、用户身份、操作系统安全策略等进行综合的监控和审计，全方位的监控操作系统的运行状态以及用户的操作行为，实现涉密信息的全程审计与跟踪。

## ● 丰富的统计报表

系统提供列表和统计图的报表输出，报表的输出支持HTML、EXCEL、PDF、RTF等四种格式。同时提供手动报表、自动报表等两种生成模式。

## ● 灵活的策略管理模式

系统提供单位策略、部门策略、主机策略、账户策略、网络策略，多种策略管理模式组合，可满足随时变化的策略管理需求。

## ● 客户端代理程序安装部署方式灵活、多样

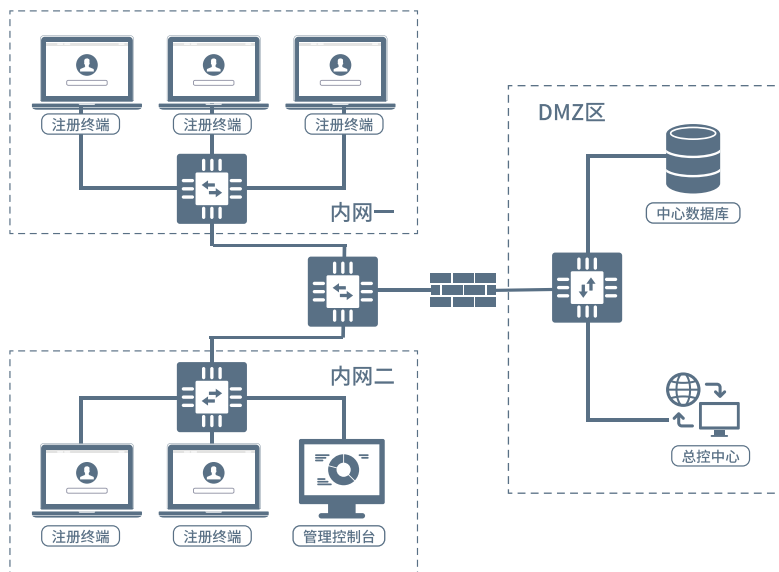
客户端代理程序同时支持域模式安装、本地安装、网络分发安装以及WEB安装等多种安装部署方式，用户可以根据实际网络环境自由选择。

## 产品部署

### ● 本地部署

本地部署是本系统最常见的部署方式，适用于对所有终端计算机进行集中管理的用户环境。在该部署方式下，所有的计算机终端注册到同一个总控中心。

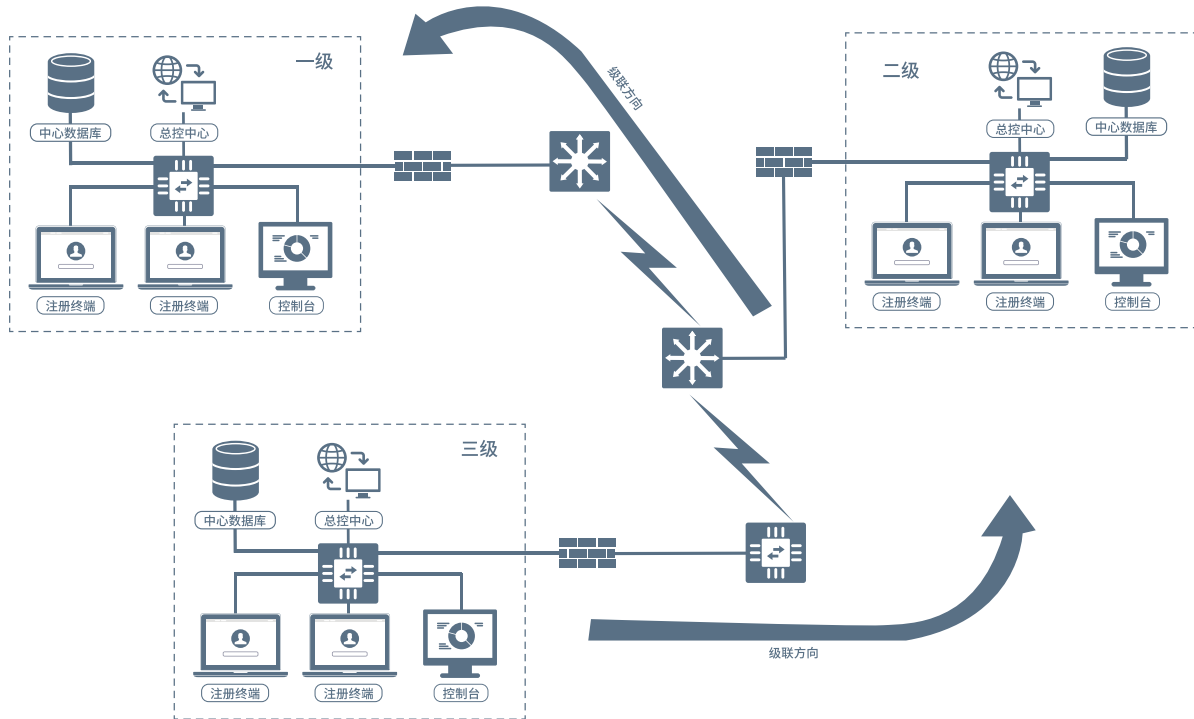
本地部署的优点是可以在一个系统管理中心监控到内网中所有计算机的活动状况。



## ● 分级部署

分级部署是指按照不同地域或者部门的不同，在内网中安装多个总控中心，不同地域或者部门的计算机分别注册到不同的总控中心。

分级部署方式的优点是，可以将实际的日常运维管理权限分散到不同的部门或区域，但上级仍然可以保留对下级的管理能力。另外，通过分级部署，可以无限的增大计算机管理数量。



## ● 服务器运行环境

运行平台: Windows Server 2008 R2、Windows Server 2012

支持数据库: SQL Server 2008 R2/2012/2016、Mysql 5.X

推荐配置: CPU 双核3.0GHz、内存8G、硬盘1T

## 用户价值

- 通过补丁分发、安全策略集中管理，保障系统运行的安全可靠。
- 对主机外设接口、移动介质进行安全管控，有效防止信息泄密。
- 通过私有端口、加密信道远程运维主机，使维护更安全、快捷。

地址: 北京市海淀区高梁桥斜街 59 号院 2 号楼 3 层 / 邮编: 100044 / 技术支持热线: 800-810-2332 / 400-966-2332

电话: 010-82138088 / 技术支持邮箱: support@sbr-info.com / 网址: www.sbr-info.com