JUMING 聚铭
让安全更简单

# 聚铭安全产品

EASIER WAY FOR SECURITY

累计服务10000+政企客户

# 聚铭终端安全管理系统
# (AV)

聚铭网络
www.juminfo.com

# 聚铭终端安全管理系统（AV）

终端卫士 智净威胁


## 需求痛点

1

### 勒索和攻击事件频发

“勒索软件即服务”、“双重勒索”等攻击手段层出不穷，全球企业和组织面临前所未有的安全挑战。

2

### 网络边界模糊

随着远程办公、云视频会议等应用爆发，作为承载业务和数据的终端、服务器系统成为新的高风险点。

3

### 主机安全管理复杂

不同操作系统和计算平台的存在使得统一管理成为难题，加大了事后追踪的难度。

4

### 监管合规要求

《网络安全法》、关基条例等政策法规对终端安全防护提出了严格要求，需满足行业监管。

# 聚铭终端安全管理系统

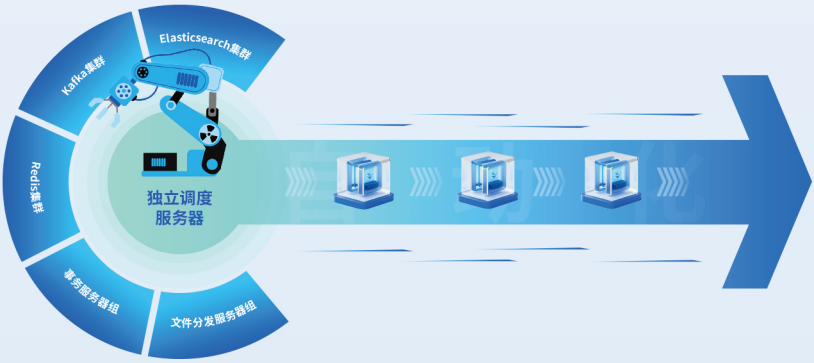
## 一站式终端安全解决方案

聚铭终端安全管理系统是一款智能防护终端、服务器、虚拟机、云主机和信创环境安全的新一代全栈主机安全产品。产品集防病毒、EDR、桌面管理、数据防泄漏、入侵防御、微隔离、资产清点、虚拟补丁等功能于一体，兼容不同操作系统和计算平台，基于单一代理、单一管理控制台帮助客户建立面向已知和未知威胁防护以及统一管控、高效运维的新一代主机安全立体防护体系。


# 产品亮点

## 高可用、可伸缩的系统架构

系统采用Elasticsearch、Kafka、Redis集群及事务、文件分发服务器组，并通过独立调度服务器实现自动化资源调度。单个服务器故障不影响整体，支持无限扩展，具备高可用、可伸缩、低耦合和低故障率特点，灵活管理从几百台到上百万台主机。



## 智能、轻量、高安全代理

02

利用静态风险分析、动态行为监控和机器学习技术，减少对文件监控的依赖，降低系统性能影响。代理端自适应调度，优化多核利用和并行计算，以轻量级资源占用实现高效安全防护，有效识别和预防已知及未知威胁。

## 勒索病毒围猎矩阵

03

针对勒索病毒，在常规防御基础上，从静态和动态两维度定制全生命周期围猎矩阵。静态防御使用专用AI模型增强检测；动态防御通过行为狩猎捕捉危险行为，如删除卷影、关闭修复，并用勒索诱捕识别可疑操作，全面覆盖预防、检测和响应各阶段。


## 国产自主人工智能引擎

04

系统内置Protoss™引擎，代表国产杀毒引擎顶尖水平。它利用海量恶意样本和高质量训练，结合机器学习，精准预测和阻止恶意代码。相比传统引擎，Protoss™检测率更高、资源占用更低、扫描速度更快，适用于终端和网络侧的大批量文件扫描。


## 强大的数据采集和检测

05

基于终端内核态采集（覆盖Win/Linux的20大类60+子项），依托终端安全大数据平台，通过自定义进程ID关联分析攻击步骤，以图形展现完整攻击场景，将复杂的安全数据流结构化，帮助管理员洞悉攻击策略、意图及预测后续行为，实现高效应急响应。

## 全面支持信创生态

系统全面支持信创生态，支持银河麒麟、中标麒麟、深度、UOS、中科方德、红旗等国产操作系统，支持兆芯、飞腾、海光、鲲鹏、申威、龙芯等国产CPU，可实现信创终端和非信创终端统一集中管理，有效满足国产信创终端防病毒需求。


## 支持零信任联动

系统全面支持零信任联动，感知并度量主机环境，主动推送变更至安全策略控制，核查网络环境、恶意代码、漏洞、系统配置、应用环境及健康项风险，保障主机安全。

# 产品价值

### 降低企业安全风险

有效抵御主机面临的已知与未知威胁，保护关键业务和数据安全，减少企业遭受攻击的风险。

### 提升主机运维效率

通过单一控制台实现多任务统一管理（杀毒、修复、管控等），简化主机运维流程，提高工作效率。

### 事件溯源快速响应

提供强大的监控和数据采集功能，能够全面记录安全事件，并支持快速检索和识别受影响的主机，加快应急响应速度。

### 覆盖全栈终端安全

适用于多种环境（包括物理机、虚拟机、云主机等）和应用场景的全栈安全解决方案，集成网络防病毒、EDR、服务器安全管理多重功能，避免堆砌产品。

聚铭 juminc

聚铭订阅号

荣获国家发明专利20余项
通过【ISO9001质量管理体系认证】【ISO27001信息安全管理体系认证】
【ISO20000信息技术服务管理体系认证】【CCRC信息安全风险评估服务资质认证】
【CCRC信息安全应急处理服务资质认证】

公司地址：江苏省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　　传真：025-52205565
全国统一服务热线：400-1158-400　　公司官网：www.juminfo.com