金山安全
Kingsoft Security

新一代 一站式终端安全管理平台

终端安全系统V9

精于病毒防御 统管终端安全

终端安全管理系统 V9.0
www.ejinshan.net

金山安全是国内领先的云安全与 SaaS 服务提供商，以“全面保障数字化环境安全”为企业使命，协助政府、军队、大型集团化企业和专用网络等企事业单位，构建专属的信息安全保障体系；为小型企业提供 SaaS 化的安全及泛安全产品与服务。

金山安全是在金山已运营 10 年之久的企业安全业务基础上实现的独立运营，是拥有完全自主知识产权的中国信息安全企业。

目前，金山安全已为数十万的客户群体和上千万的终端用户提供产品与服务，在包括政府、大中型企业、公安、军队等客户中拥有良好的口碑。无论终端安全防护、网关威胁预警、专用业务系统加固还是桌面安全管理、未知威胁检测，金山安全均为用户提供业界最领先的安全产品和专业服务，及提供立体化安全整体解决方案。

公司使命：全面保障数字化环境安全

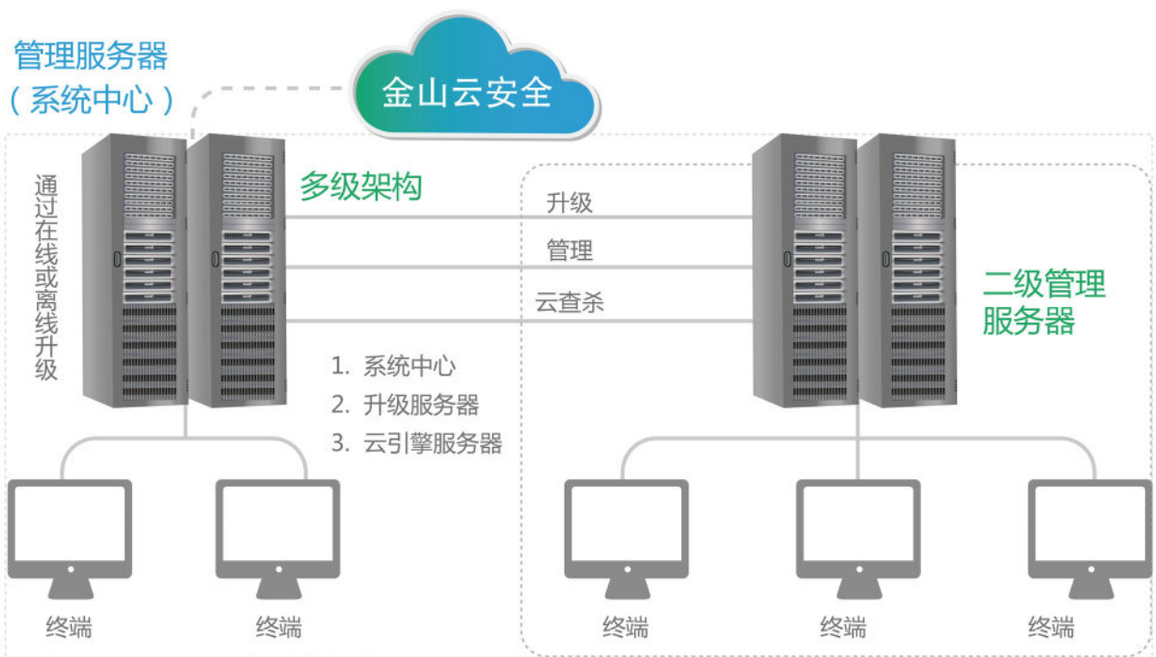
公司定位：云安全与 SaaS 服务提供商

产品说明

金山终端安全系统 V9.0 是专门为政府、军工、能源、教育、医疗及集团化企业设计的终端安全管理平台，是根据多年来市场需求及安全威胁的不断快速迭代，V9.0 是在 V8.5 基础上的全面升级，集成了恶意代码快速查杀、安全攻击实时防护、全方位桌面管理、丰富的运维支撑、灵活的漏洞补丁管理、细粒度的外设管控以及多维度的日志审计回溯等功能，增强了包括从异常检测、行为安全管控、安全加固、安全运维及安全事件回溯等维度实现终端整体安全防护，是一款一站式终端安全管理 EDR 产品。

金山安全持续利用最新技术，以大数据为基础驱动，集中分析终端安全数据；机器学习智能安全检测，通过高效算法精准识别、全程跟踪及快速响应安全威胁；体系化产品设计理念，构建包括本地、边界再到云端的立体式防护体系。产品理念上创新，研发技术上领先，以应对层出不穷的安全新威胁。

通过金山终端安全系统 V9.0，协助用户实现对终端从接入发现、使用管理到退网结束的安全风险全生命周期管理，打造包括威胁发现、分析、响应及回溯等全链路跟踪的解决方案。实现在病毒高效防御基础上统一管理全网终端安全，达到终端安全工作可管可控可审可视效果。



产品功能

帮助企业提升终端安全管理水平，建立高效主动防御体系，有效防范病毒感染、漏洞攻击及未知威胁，通过整体统一管控，规范终端使用行为，减少网络资源滥用，降低敏感数据泄漏风险，确保企业内网安全合法合规。通过一键式远程维护及外设管控策略，大幅提升运维工作效率，全量安全行为审计回溯，实现安全可视化，为安全事件追踪、数据取证、风险加固工作提供数据依据。

恶意代码实时查杀

系统集成了“云启发引擎 3”、“蓝芯 III”及“小 U 本地引擎”等多引擎技术，终端资源消耗优势行业领先。同时内置了已申请专利基于 HIPS 的勒索者主动防御机制，蠕虫病毒、勒索病毒、宏病毒等的已知未知威胁防范无忧。

安全攻击立体防护

囊括了云端、本地及边界的全方位主动防御体系，能够精准识别、分析及响应病毒传播、0day 攻击及 APT 攻击等异常行为。同时通过 XP 防护盾，强化针对 WINDOWS XP 的特有保护，支持 windows、linux、国产操作系统、虚拟端及移动端 ,避免安全盲区。

灵活的漏洞补丁管理

快速掌握全网终端漏洞及补丁修复情况，可制订包括流量、时段及范围等的灵活升级策略，支持对补丁进行升级前验证，减少升级异常机率。

全方位的桌面管理

全网终端资产自动识别，实时跟踪资产变化；软件进程化集中管理，避免不明软件带来的安全风险；流量严格管理，避免网络资源滥用；网络访问黑白名单管控，规范终端安全使用，进而减少安全风险。

丰富的运维支撑

远程桌面登录维护以及文件快速分发，提高运维工作效率；通过单点维护能力，实现终端的服务、账号、网络、共享及进程等管理一键式运维支撑。

细粒度的外设管控

可按接口类型及外设类型进行管理，有效管控常用外设使用，杜绝非法外联。支持 U 盘注册、加密及验证管控，避免外设混用、私用及乱用，有效降低数据泄漏及病毒感染风险。

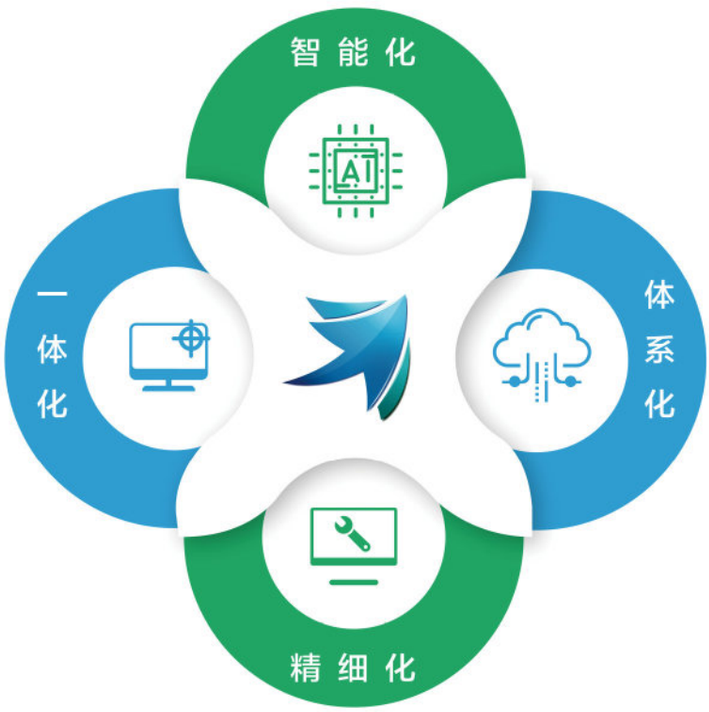
多维度的日志审计

实时收集全网终端病毒查杀、漏洞补丁、外设使用、软件使用、终端行为等全量日志，通过多维度进行关联、持续分析，有效挖掘隐藏威胁，实现终端安全事件溯源、可视。

产品特点

平台框架智能化

数据统一深度分析　　人工智能高效检测
未知威胁自动识别　　全程追踪安全可视



终端运维一体化

系统一键加固
全量日志收集
文件统一分发
远程维护支撑

安全保障体系化

“云+端+边界”保护
多引擎联合主动防御
多样化立体防护手段
全系列操作系统支持

桌面管理精细化

全网资产统一管理　　终端行为可管可控
软件进程精准管理　　外设管理一步到位

产品价值

全网终端统一管控
终端安全一体化管理

协助企业全网终端安全管理 all in one，实现终端安全、行为及维护支撑等统一管理。

精细化感知网络威胁能力
识别未知威胁攻击

全面监视系统中所有进程活动，准确识别并拦截新型恶意程序，通过大数据持续分析跟踪异常行为，有效防范 APT 攻击。

构筑云 + 边界 + 端
的立体式主动防御体系

实现从私有云端、网络边界、服务器端到终端的立体防御。与其它安全设备无逢联动 ,打造深层次的防御体系。

全面管控终端
实现高效运维

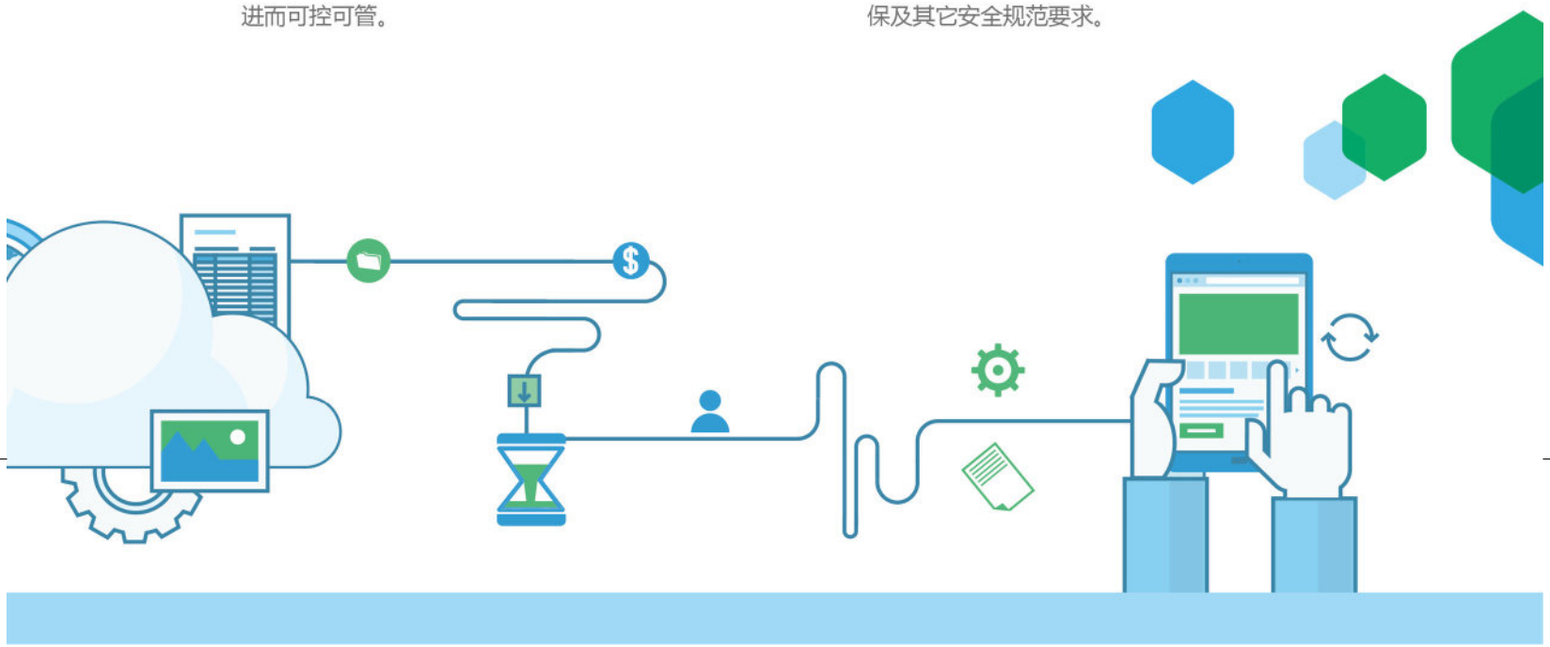
具备终端资产、软件使用、终端行为及流量管控等强大的终端管理功能，规范终端使用行为。同时提供丰富运维能力，提高运维工作效率。

终端安全事件行为审计回溯
实现安全可视化

让不可易见的“暗箱操作”安全事件，变成“透明可见”，实现对安全可见，进而可控可管。

协助企业终端
管理合法合规

企业的终端管理策略、安全合规策略得到合理规划及管控，满足企业内网、行业等保及其它安全规范要求。



事故溯源为安全风险
加固提供数据支撑

通过事后审计，进行事故溯源，为安全风险加固修复、安全措施完善及安全取证等提供数据支撑。

协助管理人员构建完善的
安全保障体系

全面评估内网终端安全状况，为安全保障工作决策提供指导依据，从而进一步构建完善的安全保障体系，为安全保障工作决策提供指导依据。

应用场景

终端统一安全管理

实现全网终端的病毒查杀、攻击防御、漏洞修复、软件管理、行为管控、外设管理、流量管控、远程维护等管理。

APT 攻击防御

持续威胁跟踪 ,详细日志审计 ,云、界、端立体式防御框架及与第三方无逢联动对接 ,让隐藏的APT 攻击一鉴无余。

勒索型病毒防御

勒索病毒主动防御机制，漏洞一键全网修复，严格外设管控，邮件、下载及共享等边界实时监控，有效防范勒索病毒及其变种威胁。

内网安全环境保障

恶意代码实时防御，规范内网终端使用，外设严格管理，保证内网环境安全，降低数据泄漏及破坏、业务中断风险。

等保合规

企业的终端管理策略、安全合规策略得到合理规划及管控，满足各行业安全规范要求。

内网安全统一评估

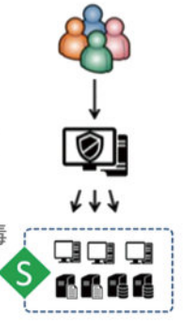
全面的内网安全评估，快速掌握内网安全健康状况，为安全保障工作决策提供指导依据。

LINUX信创专用版

产品说明

金山终端安全系统V9.0（Linux信创版）是专门为政府、军工、能源、金融、医疗及其他集团化企业设计的基于Linux操作平台的终端安全管理系统。金山安全在终端安全领导型产品V9.0的基础上独立分割并全新研发的Linux信创版，是基于多年来对安全威胁的防御经验及市场需求的把握，遵照了信息化创新发展的技术要求， 实现了对Linux操作系统的完美适配，全面集成了恶意代码快速查杀、安全攻击实时防护、运维支撑的丰富技术以及多维度的日志审计回溯等应用功能，是一款一站式威胁检测、响应、阻断及管理的EDR产品，可全面统管Linux终端安全。

安全技术智能化，一站式管理 的设计理念



以安全大数据为基础驱动，全网捕捉、集中分析终端安全数据。

- 检测模型智能化：机器学习的算法高效、精准，可快速识别、全程跟踪安全威胁；
- 设计理念体系化：构建本地、边界到云端的立体式防护体系；
- 威胁分析技术关联化：威胁文件与行为的多维度关联分析，能快速溯源，减少病毒重复感染；

终端管理全生命周期，从检测到响应的EDR架构

点到面管控、端到端定位！

- 协助用户实现Linux终端的威胁从接入、发现、使用管理到退网结束的安全风险全生命周期管理；
- 打造包括安全威胁从发现、分析、响应到回溯等在内的全链路跟踪处置解决方案，关联攻击链路、定位攻击源头、挖掘蛛丝马迹；
- 在病毒高效防御基础上统一管理全网终端安全，达到终端安全工作可管可控可审可视。

产品功能

01

终端全网统一管控
终端安全一体化管理

协助企业全网终端安全管理all in one，实现终端安全防御和维护支撑的统一管理。

02

构筑云+边界+端的
立体式主动防御体系

实现从私有云端、网络边界、服务器端到客户端的立体防御。与其它安全设备无逢联动，打造深层次的防御体系。

03

精细化感知网络威胁
全面识别未知威胁攻击

实时监视系统中所有进程活动，准确识别并拦截新型的未知的恶意程序，通过大数据持续分析跟踪异常行为，有效防范APT攻击。

04

终端安全行为的审计
实现全网安全性可视化

审计并回溯安全事件与行为，让“暗箱操作”的“黑手”变得“透明可见”，实现对安全的可见、可控和可管。

05

终端安全事故的溯源
为安全风险加固提供数据支撑

通过事后审计，进行事故溯源，为安全风险加固修复、安全措施完善及安全取证等提供。

06

安全保障体系的构建为安
全管理人员提供强有力工具

全面评估内网终端安全状况，为安全保障工作的决策提供指导依据，从而达成完善的安全保障体系的构建和持续优化。

亮点介绍

01 20年技术积淀 行业领先的查杀引擎

系统集成了金山安全的“蓝芯III”、“云启发引擎3”、及反勒索病毒引擎等行业领先的多引擎技术，终端资源消耗优势行业领先

- 蓝芯III引擎：包括多种算法，拥有自我学习能力，使用了金山安全火眼系统并具有流行性病毒及变种的强力分析技术，可大幅度提升防御能力并提高病毒检出率。
- 云启发引擎3：依托金山安全公有云的业内领先优势，产品的高查杀能力数倍于传统企业杀毒软件，且终端资源占用远低于传统杀软。
- 反勒索病毒引擎：内置了已申请专利并基于HIPS的勒索者主动防御机制，蠕虫病毒、勒索病毒、宏病毒等已知未知威胁防范无忧。无忧。

02 前端应用-统一管理

终端安全防御具有终端多类别、行为多样、管理繁杂琐碎等天然特征。金山终端安全系统(Linux专用版)V9.0自诞生起，便将“管理便利”定义 为用户的核心诉求， 通过批量部署、分级分层、一键分发、统一配置等便捷操作设计以达到对终端快速统一管理，便于提高系统对安全事情的响应能力。

终端统一管理

- 病毒查杀
- 统一升级
- 日志收集
- 终端维护

03 前端应用-异常警告

金山终端安全系统V9.0(Linux信创版)经过持续迭代完善， 构建了包括事前安全策略创建、事中实时管控告警及事后安全审计回溯的全生命周期安全防御体系，支持多种方式对内网安全事件进行告警，方便管理员了解全网终端安全威胁，并对安全事件进行快速跟进处理。

- 页面异常告警
- SNMP Trap通知
- E-MAIL下发告警
- 信使服务告警（WINNT平台）

04 前端应用-安全评估

通过安全防御、程序更新、终端安装等多个维度对全网终端进行统一安全评估，实时快速掌握内网安全风险状况及趋势变化，以及待处理的安全威胁。达到一键安全评估、一键修复风险，同时为内网的安全保障工作决策和指导提供数据依据。

05 前端应用-安全审计

具有强大快捷的日志审计功能，能够对攻击、病毒等终端运行信息进行统一收集、汇总并有效管理，形成图形化的审计报告。通过日志进行安全事件实时跟踪、关联分析，发现内网威胁的蛛丝马迹，全力支撑可视化回溯和数据取证。

- 页面异常告警
- SNMP Trap通知
- E-MAIL下发告警
- 信使服务告警（WINNT平台）

06 前端应用-多维报表

报表种类

终端部署、病毒查杀、安全事件等；

报表维度

支持统计、排名及走势，同时支持日、周、月、季度、年度及时段综合报表，以及分级分组报表；

报表图表

趋势图、柱状图、百分比图等。

适配证书

中标麒麟 NeoKylin





统信软件 UNIONTECH | UOS


deepin 深度科技



银河麒麟 KYLIN

龙芯中科 LOONGSON TECHNOLOGY

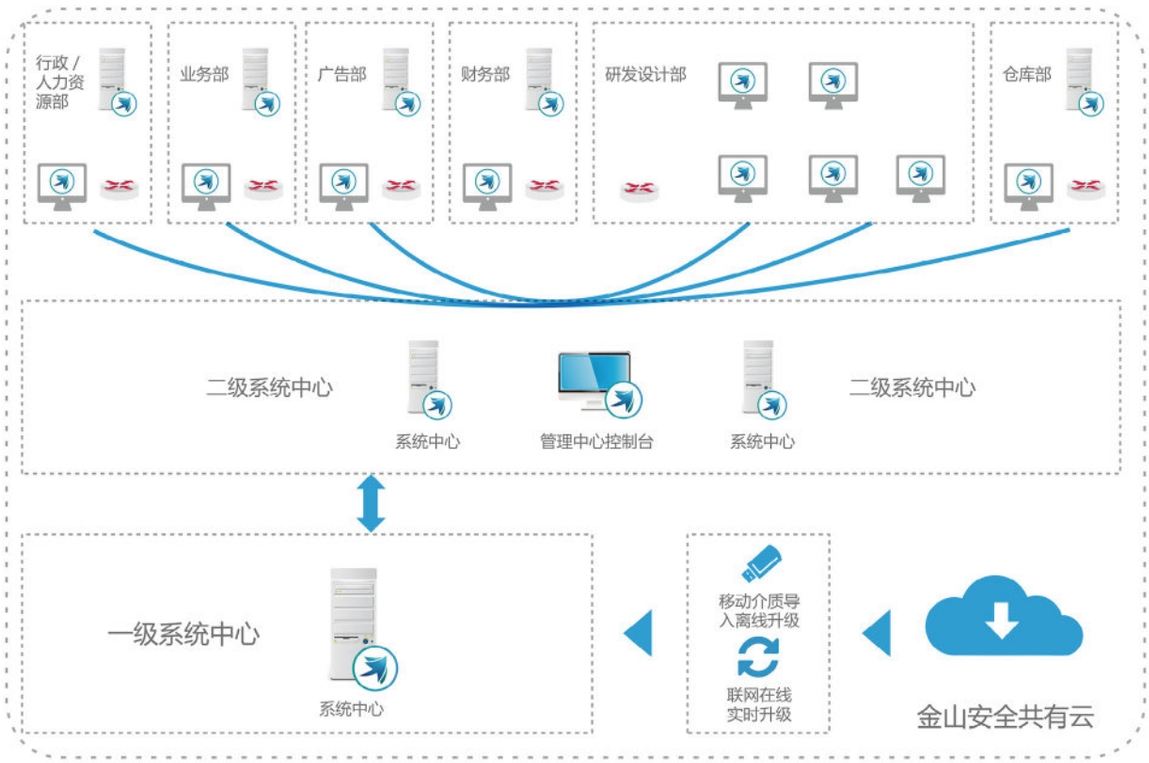
超越申泰

TRUST 100信

NewStart

产品部署

金山终端安全系统 V9.0 主要包括系统中心及客户端两部分，系统中心集成了云查杀引擎及升级服务，支持无限分级部署，满足大型多分支企事业单位如互联网、隔离网等复杂网络场景。产品使用主系统中心来集中管理数据，具有良好的可扩展性和可伸缩性，灵活快速应对网络扩容。支持页面、远程、域脚本及 EXE 打包等多种安装方式，制订终端统一快速安装策略，迅速完成全网终端安装。



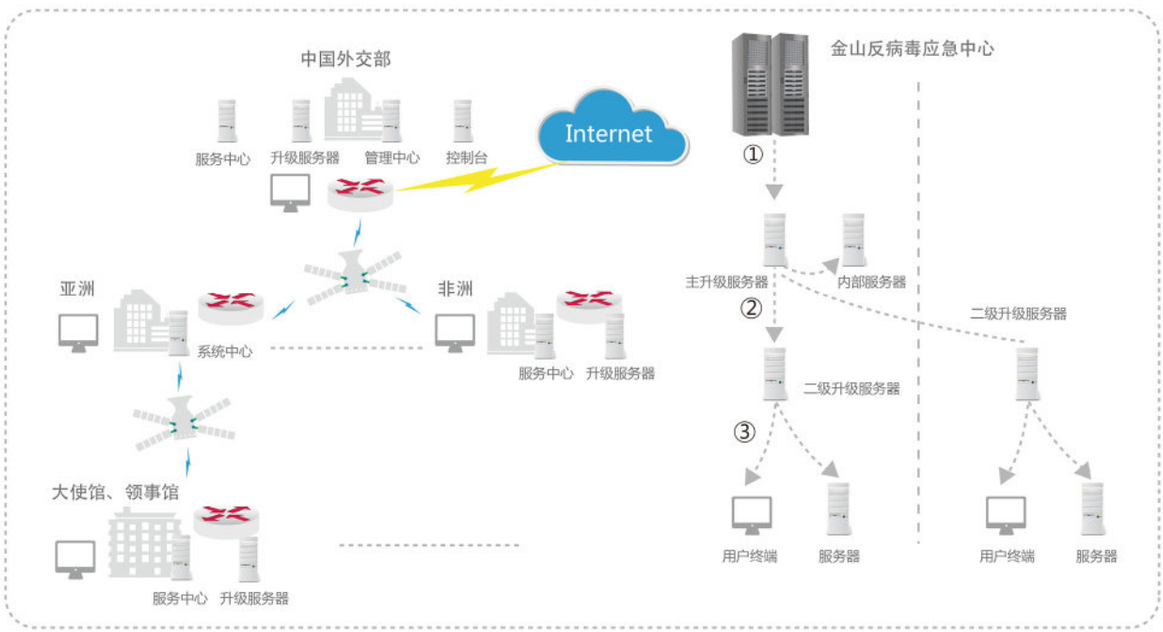
典型案例

中国外交部

——金山终端安全系统部署方案

案例概况

共部署 50 个系统中心、近 8000 客户端及近 1000 服务器端。终端遍布全球 200 多个国家，病毒种类繁多，外部政治环境复杂。实现全球终端统一安全管控，协助维护国家层面安全。

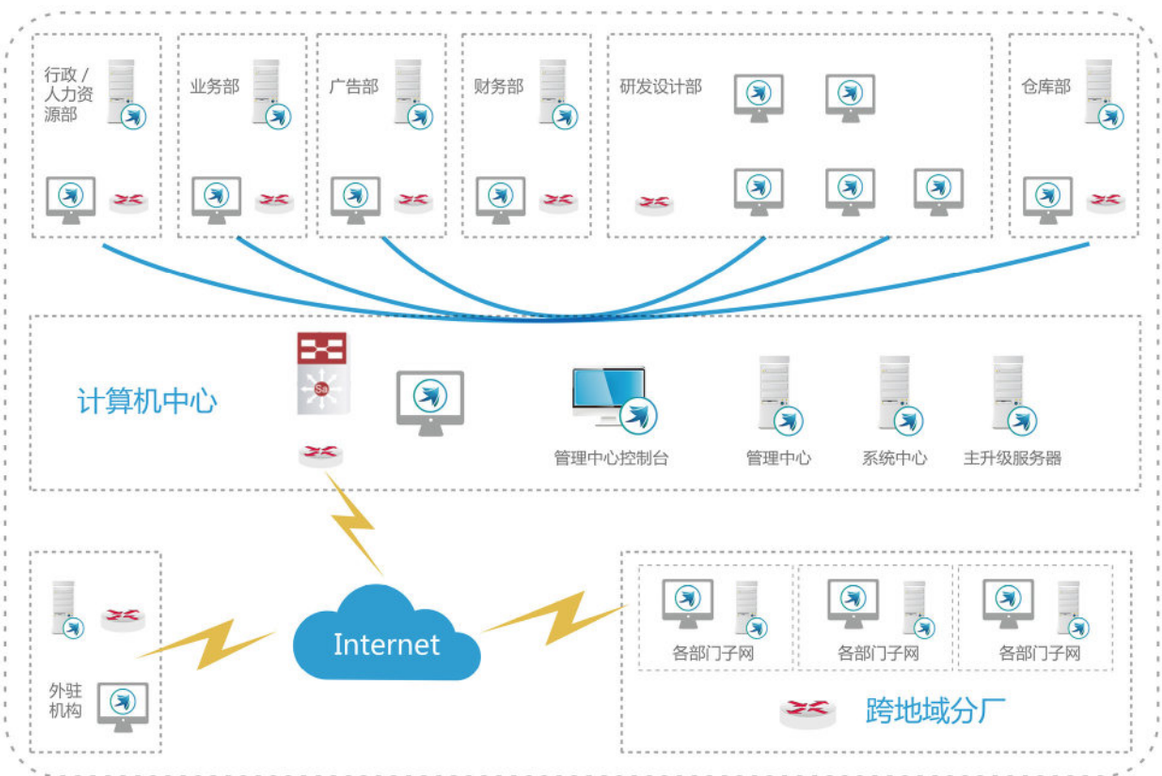


中国进出口银行

——金山终端安全系统部署方案

案例概况

共部署 66 个系统中心、近 6000 客户端及近 600 点服务器端。构造云端、边界到端点的立体式安全防御体系，捕捉任一角落威胁，实时防范通过 0day 及 APT 等攻击盗取或破坏银行业务数据。

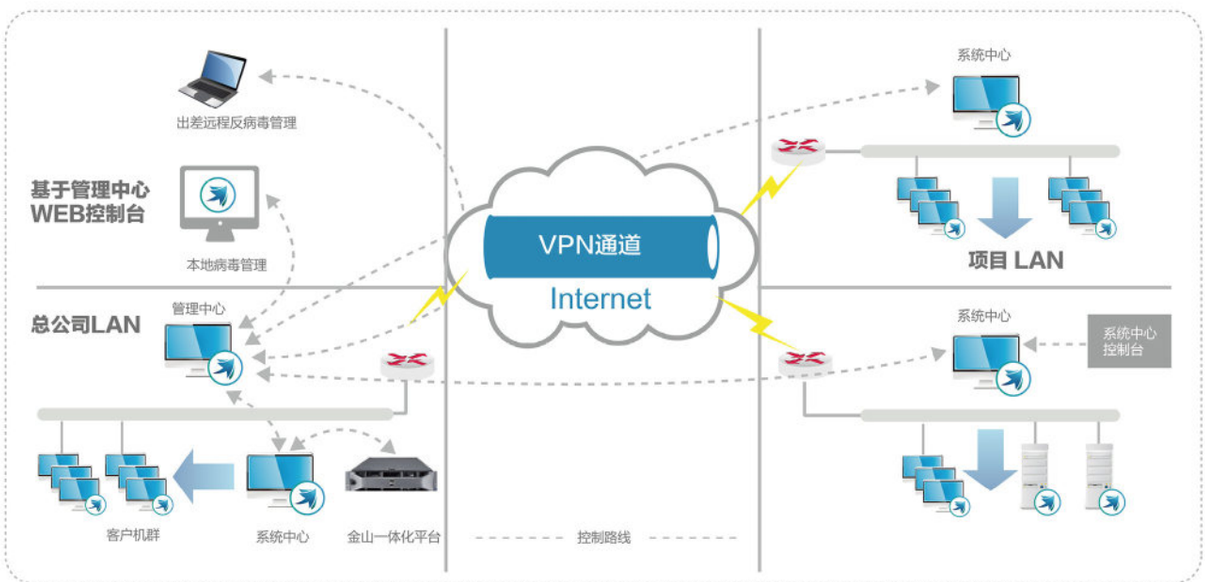


国家电力投资集团

——金山终端安全系统部署方案

案例概况

共部署 400 个系统中心、60000 多客户端及 10000 多服务器端。实时对总部、分支机构、基地及各项目工程部局域网终端进行安全保障。区域跨度极大，满足一站式灵活部署及管理。

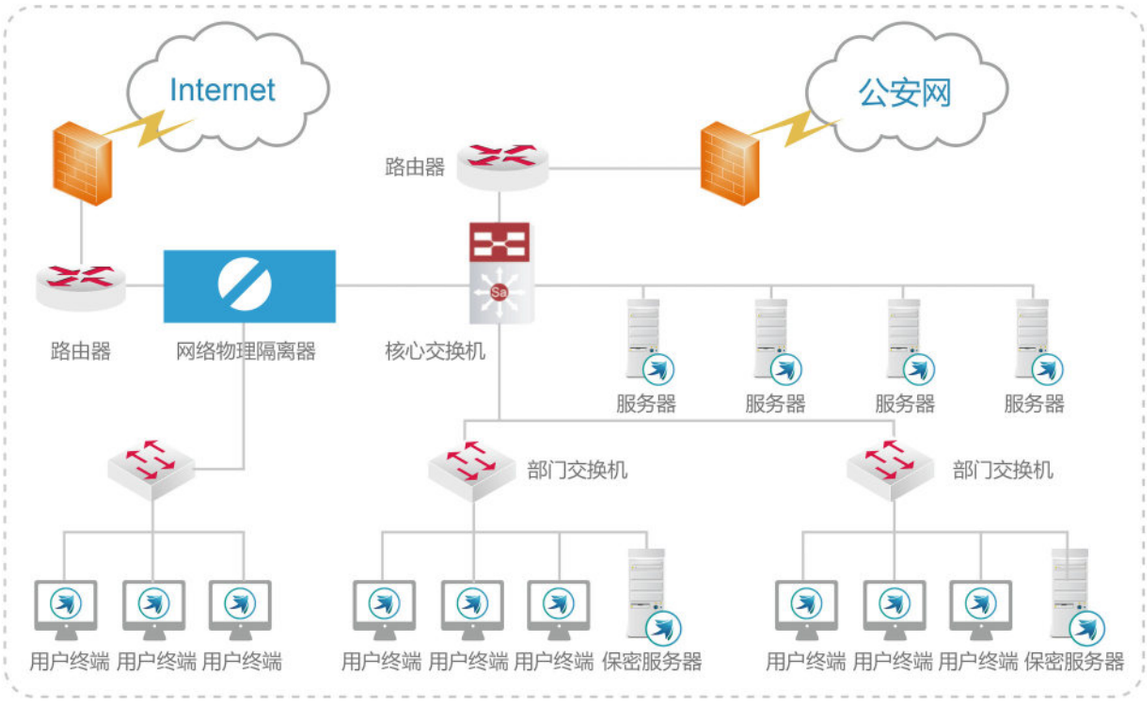


山西省公安厅

——金山终端安全系统部署方案

案例概况

共部署 15 个系统中心、80000 多客户端及 10000 多服务器端。对全省、市、县等公安网点终端进行安全保障，有效防御各种已知、未知威胁，杜绝核心绝密数据遭受泄漏及破坏。



政府及重要事业单位

中国外交部
中国农业部
国土资源部
国家保密局
国家海洋局
国家新闻出版总署
中国科学院计算机网络信息中心
广东省人民政府
济南军区政治部
四川省卫生厅
.....

军队/公安/保密等机构

福建省司法厅
四川省司法厅
山西省公安厅
黑龙江省公安厅
新疆维吾尔自治区公安厅
湖北省人民检察院
广东省人民检察院
黑龙江省人民检察院
海南省高级人民法院
贵州省高级人民法院
.....

专业业务网络

中国农业科学院农业信息研究所
中国兵器工业第五九研究所
中国科学院半导体研究所
中国民用航空总局第二研究所
广东省司法警察医院
河北省人民医院
湖北省直属机关医院
黑龙江省武警总队医院
河南省胸科医院
河南省儿童医院
.....

大型企业集团

国家电力投资集团公司
中国海洋石油总公司
中国电子科技集团公司
中国出版集团公司
国核工程有限公司
中国移动通信集团重庆有限公司
浪潮云服务信息科技有限公司
红塔烟草（集团）有限责任公司
厦门市美亚柏科信息股份有限公司
步步高集团
.....

金山终端安全系统V9.0在政府、军工、专业业务网络及大型集团企业等领域，成功护航上百万数量级的企业客户，帮助他们构建了安全的信息化环境。

所获认证

20 次通过 VB100
国际权威认证

英国西海岸三项
国际认证

国际 AV-C 测试扫描
速度世界领先

军队认证

公安部认证

国内首家微软病毒
信息联盟成员

国内首家荣获
三个黄标认证

公安信息网络安全及
“一带一路”峰会安全保障单位

第 13 届全运会安全
保障支撑单位

金砖国家领导人会晤
安全保障支撑单位

全方位一站式服务体系

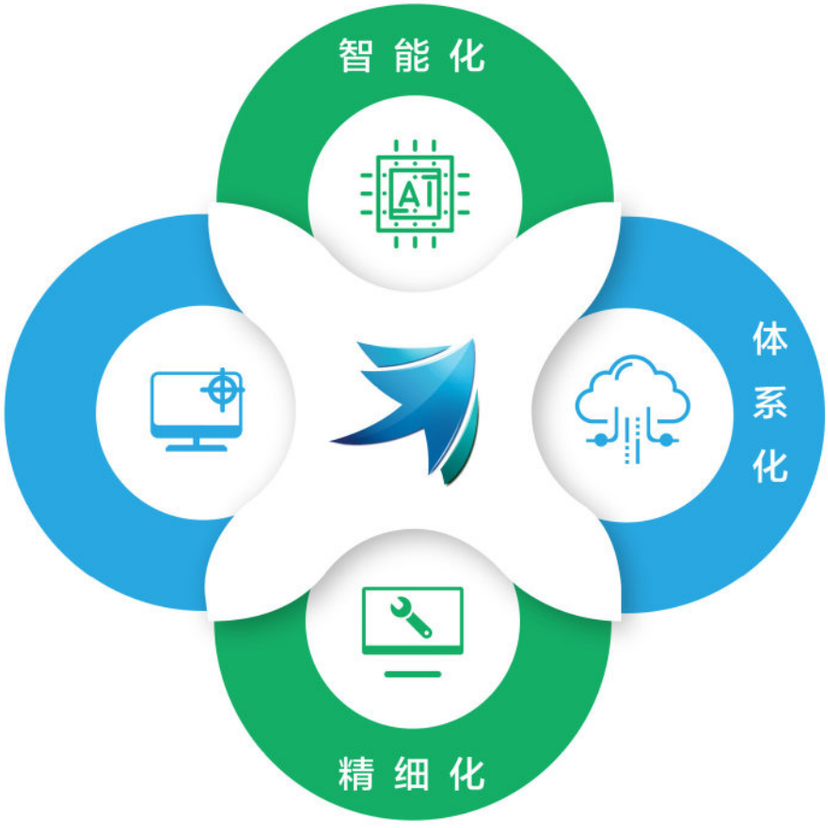
金山终端安全系统 V9.0 通过在安装部署、运营维护、预警回访、专业培训四个方面，让企业级用户充分享受专业一站式服务的全面、精确、快速的优势，进而为客户创造价值。

金山安全服务承诺：

- 全方位
- 实时
- 专业

金山安全服务目标：

- 安全风险全面掌控
- 全面节省管理成本
- 加强用户安全运维能力



金山安全
Kingsoft Security

地址：北京市朝阳区北三环东路三十号中国建筑科学研究院新办公楼12B 100013
传真：010-82663885 网址：www.ejinshan.net 服务热线：400-033-9009

官方微信二维码