聚铭终端安全管理系统
产品白皮书

聚铭网络科技有限公司

目 录

产品白皮书 I
声明 2
联系信息 3
1. 产品定位 4
2. 设计理念 4
3. 聚铭终端安全管理系统介绍 5
3.1. 产品概述 5
3.2. 系统架构 6
3.3. 组成模块 7
3.4. 主要功能 7
3.4.1. 防病毒 7
3.4.2. EDR 9
3.4.3. 桌面管理 10
3.4.4. 主机运维 11
3.4.5. 数据防泄漏 11
3.4.6. 入侵防御 12
3.4.7. 资产清点 13
3.4.8. 虚拟补丁 13
3.4.9. 功能列表 14
3.5. 产品优势 17
3.5.1. 高可用、可伸缩的系统架构 17
3.5.2. 智能、轻量、高安全代理 17
3.5.3. 内置勒索病毒围猎矩阵 17
3.5.4. 内置下一代人工智能引擎 Protoss™ 18
3.5.5. 强大的持续采集和检测能力 19
3.5.6. 全面支持信创生态 19
3.5.7. 支持零信任联动 19
3.6. 使用环境 20
4. 产品价值 22

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和北京聚铭信安科技有限公司。

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

1. 产品定位

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终端安全产品，依托多年的安全实践和经验积累，以安全大数据、云计算、人工智能引擎、威胁情报、检测与响应等新技术为支撑，采用基因特征引擎、Protoss™人工智能引擎、云查杀引擎、行为检测引擎、终端检测与响应等威胁检测引擎，帮助政企用户快速掌控全网终端安全状态，快速处置安全问题，有效保障全网终端安全。

2. 设计理念

- 全栈解决方案

聚铭终端安全管理系统覆盖终端、服务器、虚拟机、云主机及信创环境各种应用场景，产品核心功能覆盖网络防病毒、终端检测与响应（EDR）、聚铭终端安全管理系统（EPP）、终端安全信创版、服务器安全管理系统等产品的指标，通过单个产品实现终端安全全场景、全功能、全覆盖。

- 一站式终端安全解决方案

聚铭终端安全管理系统为用户提供终端安全一站式安全解决方案，以单一代理、单一管理控制台提供恶意代码防御、漏洞修复、检测与响应（EDR）、桌面管控、数据防泄漏等多个安全功能，管理员可通过控制台对全网主机进行统一管控，包括全网威胁监测、统一杀毒、统一漏洞修复、统一策略分发、统一桌面管控、统一设置屏幕水印、统一升级等多种管理功能，极大提升了全网主机的安全可见性和管理的便捷性。

- 全方位入侵防御能力

聚铭终端安全管理系统综合采用行为分析、内存加固、虚拟补丁等核心技术，精准检测和拦截终端侧和网络侧无文件攻击、远程溢出、内网横向入侵、暴力破解等各类攻击行为。

- 以 NGAV 和 EDR 为核心，向下一代终端安全演进

下一代防病毒（NGAV，Next Generation AntiVirus）利用行为分析与机器学习来防御勒索软件、无文件攻击等高级威胁。终端检测与响应（EDR，Endpoint

Detection and Response）通过对终端行为的全面监控与数据采集，基于机器学习和关联分析技术来发现安全威胁，自动实现攻击阻止、隔离修复、取证分析和追踪溯源。聚铭终端安全管理系统内置 NGAV 和 EDR 两大下一代终端安全核心组件，结合基因特征引擎、云查杀引擎、主动防御等传统防病毒技术，从容应对各种已知和未知安全威胁。

- “四引擎”实现强大的查杀能力

内置包含基因特征引擎、人工智能引擎、行为检测引擎、云查杀引擎的“四引擎”架构，实现多杀毒引擎间优势互补，对已知和未知病毒、在线和离线均具备超强的查杀能力，支持对勒索病毒、挖矿木马、蠕虫病毒、引导区病毒等恶意代码进行有效查杀。

- 追求“更轻、更快、更强”

聚铭终端安全管理系统采用静态风险特征分析、动态行为序列分析、机器学习、主机行为的全面监控与数据采集等先进技术，充分发挥人工智能模型强大的泛化检测能力、充分发挥机器学习算法在多核利用、并行计算、占用资源可控、跨平台兼容等方面的优势，减少对传统防病毒的文件监控和特征库的依赖，相比于传统终端安全产品具有更轻、更快、更强的特点。

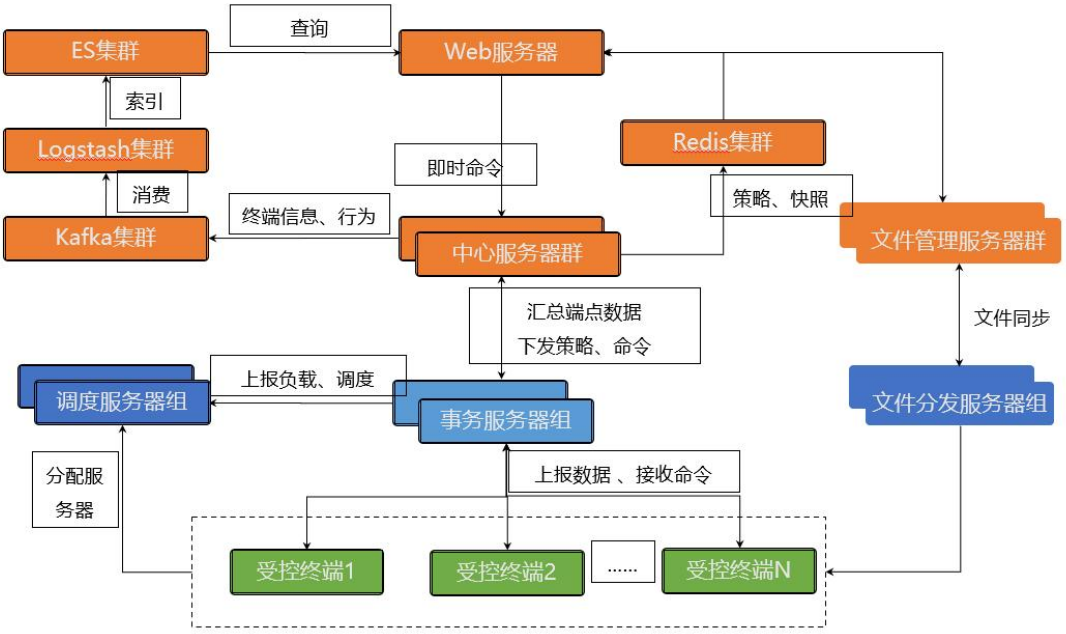
3. 聚铭终端安全管理系统介绍

3.1. 产品概述

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终端安全产品，该产品集防病毒、EDR、桌面管理、数据防泄漏、入侵防御、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、高效运维的新一代终端安全立体防护体系。

3.2. 系统架构

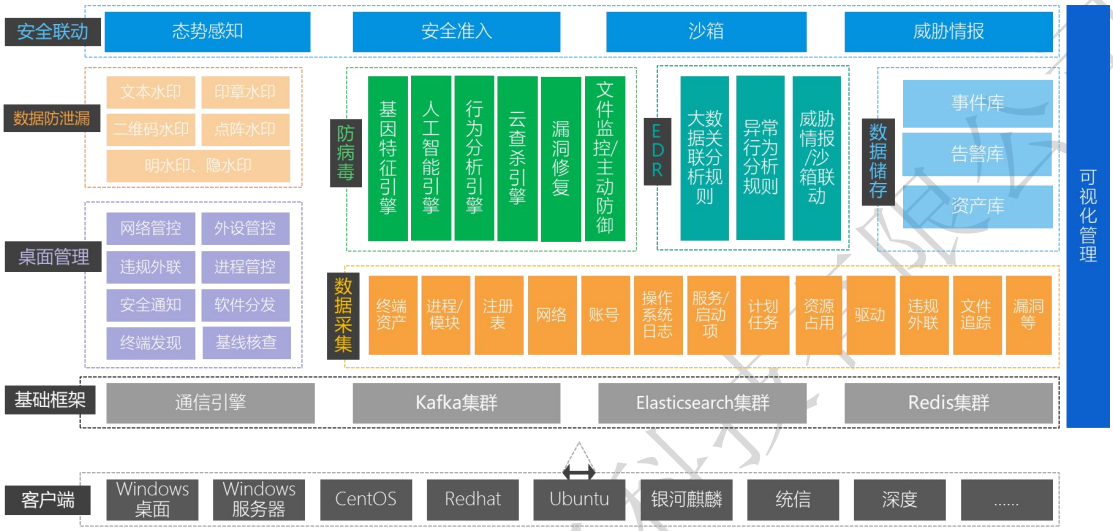
聚铭终端安全管理系统分为管理服务器（中心服务器、节点服务器）和受控主机代理两部分组成：



- 管理服务器：由中心服务器和节点服务器组成，其中中心服务器由 Elasticsearch 集群、kafka 集群、Redis 集群、WEB 服务器等组成，实现对所有主机的统一管理，包括全网主机监控状况监测、分组管理、策略制定与下发、安全巡检、软件升级管理等。节点服务器由调度、事务服务器、文件分发等服务器组成，主要作用是负责与受控主机代理进行通信，在系统架构中起承上启下的作用，将中心服务器的策略、命令、升级包转发至受控主机，将受控主机采集的信息、工作状态上报至中心服务器。
- 受控主机代理：部署在受保护的终端、服务器或虚拟机上，执行最终的病毒查杀、漏洞修复、信息采集、屏幕水印、威胁发现等安全功能，并可根据控制中心下发的安全策略执行相关安全防护动作。

3.3. 组成模块

聚铭终端安全管理系统由客户端、基础框架、功能模块（包含防病毒、EDR、桌面管理、数据防泄漏、数据采集、入侵防御、虚拟补丁等）、数据储存、安全联动、可视化管理等模块组成，如下图所示：



3.4. 主要功能

3.4.1. 防病毒

聚铭终端安全管理系统内置基因特征引擎、人工智能引擎、行为检测引擎、云查杀引擎的“四引擎”架构，完全自主知识产权，处于国内领先水平，融合机器学习、行为分析、威胁情报等关键技术，可检测各类已知和未知威胁，全面赋予终端主动安全防御能力。

3.4.1.1. 基因特征引擎

基因特征引擎负责处理复杂的、多变的、顽固的并且具有感染性的病毒，具有很强的启发性和通杀性。主要功能模块包含：

特征匹配引擎：应用最广泛的广谱查杀引擎，可以针多种加壳病毒进行脱壳，支持 30 多多种压缩格式检测，支持感染式病毒的清理等操作；

脚本检测引擎：脚本类病毒专用检测引擎，支持的脚本类型包括：js、vbs、sh、python、php、html、bat、perl、lua、ruby 等等，支持多字节和 unicode 编码格式的脚本；

宏病毒检测引擎：针对 Office 病毒的专杀和清理引擎，宏病毒检测引擎支持对感染宏病毒的文档进行检测和修复；

启发式检测引擎：用于检测未知恶意代码威胁，提取待扫描对象的动静态信息，通过启发式算法评估其恶意性；

虚拟机检测引擎：用于虚拟执行检测已知和未知恶意代码威胁，将代码仿真技术运用恶意威胁检测，通过尝试仿真真实主机的所有指令，使得在虚拟机程序中模拟实体主机所有行为，从而欺骗恶意代码动态执行代码，并得到恶意代码最终的执行结果而不必承担恶意代码运行的风险。

3.4.1.2. Protoss™人工智能引擎

Protoss™人工智能引擎是基于多年在防病毒领域和数据科学方面的积累和经验独立自主研发，完全拥有自主知识产权，是自主创新和突破颠覆性技术的典范，技术水平处于国内领先水平，与传统特征引擎相比，AI 引擎的强项在于泛化检测能力，体现在对未知病毒检测率远远超过特征引擎，同时在资源占用、扫描速度等方面具有优势。

3.4.1.3. 行为分析引擎

与静态分析不同，行为分析引擎关注已经运行的进程攻击行为的发生，行为分析引擎通过对单个进程的内核态行为数据（包括进程/文件/注册表/网络/日志等）关联分析来检测与拦截攻击行为，将庞杂、无序的安全数据流转换为易于理解的攻击步骤序列图，专门用于对抗无文件攻击、PowerShell 恶意脚本、VBScript 恶意脚本、Office/PDF/浏览器/播放器缓冲区溢出、勒索病毒危险行为、挖矿行为等高级威胁。

3.4.1.4. 云查杀引擎

云查杀引擎依托云端海量威胁情报数据提升自身查杀能力，目前威胁情报中心后台有数亿条高质量威胁情报，并且云端 7*24 小时持续不间断生产新的威胁情报。云查杀引擎对于简单的、变动小的、不具备感染性的、反复出现的但是数量庞大的病毒具有较好的查杀能力，是基因特征引擎和人工智能引擎的补充。云查杀引擎支持连接互联网威胁情报中心和推送核心威胁情报至本地两种工作模式。

3.4.2. EDR

3.4.2.1. 数据采集

数据采集和分析是终端检测与响应（EDR）的核心功能，终端采集的各类安全运行数据是防御、检测和响应的重要依据，聚铭终端安全管理系统提供对终端行为的全面监控与数据采集，包括终端进程、文件、服务、驱动、注册表、网络访问、DNS 访问、HTTP/HTTPS 访问、计划任务、帐户变更等。数据采集模块工作于操作系统内核态，覆盖 Windows 和 Linux 终端行为 20 大类 60 多个子项，远超同类产品。

3.4.2.2. 攻击步骤序列图

基于上述终端强大的数据采集能力，汇聚成终端安全大数据平台，以自定义进程唯一 ID 为主线，对攻击者完整攻击行为所采用的攻击步骤进行关联分析，根据攻击事件发生的时间序列，将该次完整的攻击步骤以图形的形式展现，实现攻击场景的重构。通过攻击场景重构的关联规则以及知识的形式化表述，将庞杂、无序的安全数据流转换为结构化、易于理解的攻击场景，将反映攻击过程和意图的场景图呈现出来，从而发现攻击者的攻击策略和目的，甚至推测下一步可能的攻击行为，以便于管理员做出及时有效的应急响应。

3.4.3. 桌面管理

聚铭终端安全管理系统内置完整的桌面管理功能，提供的功能包括主机防火墙、进程管控、外设管控、违规外联检测、WIFI 外联检测、安全 U 盘、弹窗拦截、软件拦截、文件分发、远程协助、安全通告等，能够帮助用户提升终端运维效率，降低终端运维的复杂性。

3.4.3.1. 主机防火墙

提供主机防火墙功能，支持对终端端口和 IP 进行进或出单向及任意双向过滤，支持黑白名单机制。

3.4.3.2. 外设管控

提供外设管控功能，支持对终端各种外设（USB 存储、光驱、USB 外置网卡、无线网卡、蓝牙、手机、平板等）、接口（USB 接口、串口、并口、1394、PCMIA）设置使用权限，支持添加外设和端口黑白名单例外

3.4.3.3. 安全 U 盘

提供安全 U 盘功能，支持将普通 U 盘注册成安全 U 盘，企业内仅允许经过注册认可的 U 盘使用。支持设定注册 U 盘的内外网使用权限、访问密码、责任人等；支持对注册的移动介质进行管理，包括审批、撤销审批等。

3.4.3.4. 违规外联

提供违规外联监测功能，支持互联网或专网的外联探测功能，发现外联后支持设置告警、锁屏、断网等违规处理手段，支持自己搭建部署取证服务器。

3.4.3.5. 远程协助

提供远程协助功能，辅助管理员远程解决主机故障，开启远程协助不需要安装额外软件，管理员通过浏览器即可使用。

3.4.4. 主机运维

3.4.4.1. 漏洞修复

支持一键扫描 Windows 操作系统、Linux 操作系统、中间件、数据库、WEB 应用安全漏洞，支持批量修复 Windows 系统漏洞，提升安全运营效率，快速消除安全隐患。

3.4.4.2. 基线核查

基线检查是根据三级等保合规性要求对 Windows 和 Linux 操作系统的系统配置项（包括身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范等方面）进行合规性检查，辅助用户发现内网不合规终端及不合规项，对不合格项提供一键修复功能。

3.4.5. 数据防泄漏

聚铭终端安全管理系统内置屏幕水印模块，支持在敏感的屏幕内容上标记文本水印、印章水印、二维码水印和点阵水印，支持明水印和隐水印，屏幕水印关联主机名、IP、MAC、时间等信息，可以防止未经授权的屏幕截图、手机拍照、录屏，防止敏感信息泄露。

3.4.5.1. 文本水印

提供文本水印功能，支持自定义主机名、IP 地址、MAC 地址、时间作为屏幕内容水印显示，支持设置水印宽度、高度、行间距、倾斜度、水印布局等内容。

3.4.5.2. 印章水印

提供印章水印功能，支持自定义印章标题和脚注作为屏幕内容水印显示，支持设置印章半径、颜色等内容。

3.4.5.3. 二维码水印

提供二维码水印功能，支持自定义主机名、IP 地址、MAC 地址、时间作为屏幕内容水印显示，支持设置二维码大小、背景色、前景色等内容。

3.4.5.4. 点阵水印

提供点阵水印功能，支持设置点阵水印圆点半径、间隔、描边色、填充色等内容，提供单独的点阵水印检索页面。

3.4.5.5. 隐水印

文本水印、印章水印、二维码水印和点阵水印均支持设置明水印和隐水印。

3.4.6. 入侵防御

聚铭终端安全管理系统除了行为分析引擎提供的入侵防御能力之外，还提供了登录加固、异常登录、防端口扫描和防暴力破解等入侵防御手段。

3.4.6.1. 登录加固

提供登录加固功能，主要用于加固 Windows 用户登录远程桌面、Linux 用户远程 SSH，加固之后强制验证二次验证密码。

3.4.6.2. 异常登录

提供异常登录功能，对敏感时间段、敏感帐号登录 Windows 远程桌面、Linux 远程 SSH 进行告警。

3.4.6.3. 防端口扫描

提供防端口扫描功能，实时阻断对本机端口的恶意探测，防止攻击者通过扫描和嗅探获取敏感信息。

3.4.6.4. 防暴力破解

提供防暴力破解功能，可以防止攻击者通过穷举的方式获取 RDP、SMB、SSH、Telnet 敏感服务的密码。

3.4.7. 资产清点

聚铭终端安全管理系统能够帮助用户对主机内的资产进行梳理清点，杜绝未知资产，便于对全部资产进行有效防护，清点资产内容包含：操作系统、进程、服务、驱动、端口、环境变量、启动项、系统账户、口令复用、应用软件、计划任务、WEB 服务、数据库、注册表。

3.4.8. 虚拟补丁

针对操作系统漏洞、数据库组件漏洞、大数据组件漏洞、WEB 组件漏洞等提供虚拟补丁功能，在不修复漏洞的情况下拦截攻击行为，能够配置告警或拦截处置，能够配置虚拟补丁防护的终端，防止漏洞利用和提权入侵行为，漏洞利用防护告警显示漏洞 CVE 编号、主机名称、主机备注、主机 IP 地址、发生时间、攻击类型、攻击行为处置结果、攻击协议、攻击 IP 地址、被攻击主机 IP 和端口等信息。

3.4.9. 功能列表

功能点		描述
防病毒	多引擎查杀	集成基因特征引擎、Protoss™人工智能引擎、行为检测引擎、云查杀引擎多种病毒检测引擎，支持对引导区病毒、蠕虫、后门、勒索病毒、挖矿木马等恶意文件进行高效查杀
	实时监控	全面监控文件操作，实时监控支持高中低三种配置
	主动防御	提供进程防护、驱动防护、U 盘防护、ARP 防御等实时防御功能
	勒索防御	通过专用 AI 勒索模型、勒索行为分析、勒索诱捕等技术围猎勒索病毒
	挖矿防御	支持检测挖矿木马通信协议和连接矿池地址，实时阻断挖矿木马挖矿行为
	内存安全	支持无文件攻击检测、支持可疑脚本防御、支持应用程序加固
	自身安全	提供进程、文件、注册表防护，防止程序自身被破坏或篡改
EDR	持续检测	提供对终端行为的全面监控与数据采集，包括终端进程、驱动、模块、IP 访问、DNS 访问、文件操作、外设操作、打印操作、注册表变更、账户变更、操作系统日志等
	日志采集	支持采集各类 WEB、FTP、邮箱、数据库服务器日志
	攻击步骤序列图	以进程唯一 ID 为主线，对攻击者完整攻击行为所采用的攻击步骤进行关联分析，将攻击步骤以图形的形式展现，实现攻击场景的重构
	安全响应	提供多种威胁响应的方式，包括隔离文件、结束进程、隔离主机等
桌面管理	防火墙	主机防火墙支持黑名单和白名单两种工作模式，精准阻断各种非法流量
	进程管控	支持进程白名单、进程黑名单和进程红名单
	外设管控	支持对终端各种外设（USB 存储、光驱、USB 外置网卡、无线网卡、蓝牙、手机、平板等）、接口（USB 接口、串口、并口、1394、PCMIA）设置使用权限，支持添加外设和端口黑白名单例外
	安全 U 盘	支持设定注册 U 盘的内外网使用权限、访问密码、责任人等；支持对注册的移动介质进行管理，包括审批、撤销审批等
	违规外联	提供 WIFI 异常链路检测、互联网违规外联检测、专网违规外联检测等

		功能
	远程协助	提供 Windows 远程桌面和 Linux 远程 SSH
	广告拦截	提供常见软件广告拦截功能
	软件拦截	支持拦截常见捆绑软件、广告软件、各类下载器等
主机运维	安全运维	支持以任务和定时的方式对全网终端进行病毒检测与查杀、漏洞扫描与修复、基线核查与加固、安全通知和文件分发与执行
	漏洞修复	支持一键扫描 Windows 操作系统、Linux 操作系统、中间件、数据库、WEB 应用安全漏洞
	基线核查	支持根据等保合规性要求对 Windows 和 Linux 操作系统的系统配置项进行合规性检查
	弱口令扫描	支持对 Windows、Linux 操作系统进行弱口令扫描，支持自定义字典
	主机发现	通过已安装探针的主机自动发现网内未注册的主机信息，帮助用户掌握全网主机数量，以及已受控和未受控的终端范围，梳理终端安全管理边界
	异常监控	提供 CPU、内存、磁盘、流量异常检测与告警功能
数据防泄漏	文本水印	支持自定义主机名、IP 地址、MAC 地址、时间作为屏幕内容水印显示，支持设置水印宽度、高度、行间距、倾斜度、水印布局等内容
	印章水印	持自定义印章标题和脚注作为屏幕内容水印显示，支持设置印章半径、颜色等内容
	二维码水印	支持自定义主机名、IP 地址、MAC 地址、时间作为屏幕内容水印显示，支持设置二维码大小、背景色、前景色等内容
	点阵水印	支持设置点阵水印圆点半径、间隔、描边色、填充色等内容，具有单独的点阵水印检索页面
	明、隐水印	支持对文本水印、印章水印、二维码水印和点阵水印设置明水印和隐水印
入侵防御	登录加固	提供远程登录加固和本地登录加固，支持设定敏感时间段、敏感帐号、信任 IP
	异常登录	提供远程异常登录和本地异常登录告警，支持设定敏感时间段、敏感帐号、信任 IP

	防端口扫描	提供端口防扫描与自动阻断功能，支持自定义蜜罐端口和防端口扫描参数
	防暴力破解	提供对 RDP、SMB、SSH、Telnet 协议的暴力破解监视与自动阻断
资产清点	清点内容	支持对操作系统、进程、服务、驱动、端口、环境变量、启动项、系统账户、口令复用、应用软件、计划任务、WEB 服务、数据库、注册表进行资产清点
	清点策略	支持设定单项资产的清点开关、清点间隔，支持展示资产的清点状态和清点进度
虚拟补丁	漏洞防护	通过拦截主机侧网络流量中攻击数据流，实现对操作系统、WEB 组件、数据库组件、大数据组件漏洞防护
	工作模式	支持告警和拦截两种工作模式
	防护日志	记录漏洞防护的发生时间、攻击类型、攻击行为、攻击网络协议、攻击源地址等信息
外部接口	环境感知	支持对终端环境进行实时感知和度量，得出终端安全评估分数；安全评估的内容包括网络环境风险（wifi 环境）、恶意代码风险（勒索、webshell 等）、漏洞风险（严重漏洞、重要漏洞）、系统安全配置风险（未安装杀毒软件、未开启防火墙、发现管理员弱口令等）、应用环境风险（服务合规、端口合规、进程合规、软件合规）和导致终端故障的健康项（CPU/内存/磁盘/流量异常）；支持定制环境感知策略，支持设定环境感知策略执行间隔，支持批量分发环境感知策略；支持与第三方安全策略控制进行联动，支持主动推送终端环境变更、评分变更信息
	零信任联动	支持与第三方零信任代理联动，实现安全评分、联动响应
	Syslog 联动	支持与各种第三方解决方案（SIEM、综合日志）实现日志上报
	事件告警	支持自定义告警事件、告警阈值、告警方式、发送频率，支持邮箱、短信、钉钉和企业微信四种告警方式
	防火墙联动	支持与第三方防火墙联动，实现网端协同工作
	态感联动	支持与第三方态感联动，可根据 IP、DNS、MD5 等制定各类联动规则
其它	软件版本	支持内网云模式、内网多级级联等部署方式

	部署方式	支持单机、集群部署模式
	支持语言	中文（简体）、中文（繁体）、英文
	虚拟化支持	支持 VMWARE ESX、Hyper-V、XEN 和 KVM 等多种虚拟化平台部署
	IPV6	支持 IPv4/IPv6 双协议栈
	分辨率	客户端支持 1080P/2K/4K 分辨率

3.5. 产品优势

3.5.1. 高可用、可伸缩的系统架构

整体架构采用集群（Elasticsearch 集群、Kafka 集群、Redis 集群等）和服务器组（事务服务器组、文件分发服务器组等）架构设计，并单独设计调度服务器对所有服务器根据资源使用情况进行全网自动化调度，单个服务器的软硬件故障不影响系统的整体运行，系统可根据计算、存储资源使用情况进行无限扩展，保证服务器和终端始终处于最佳工作状态，整体架构具有高可用、可伸缩、低耦合、低故障的优点，可灵活支持从几百台到上百万台的主机管理规模。

3.5.2. 智能、轻量、高安全代理

借助于静态风险特征分析、动态行为序列分析、机器学习、终端行为的全面监控与数据采集等先进技术，降低传统防病毒软件对文件监控的依赖，减少文件监控对系统性能的影响，同时代理端能够根据宿主机硬件性能和资源占用情况进行自适应调度和优化，充分发挥机器学习算法在多核利用、并行计算、占用资源可控等方面的优势，保证代理端以轻量级的资源占用实现高安全防护，有效识别和预防各类已知和未知威胁。

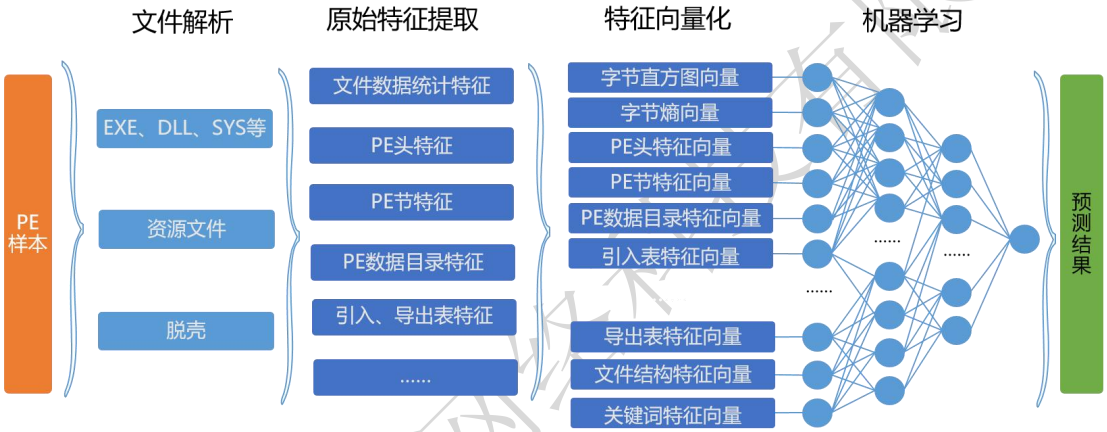
3.5.3. 内置勒索病毒围猎矩阵

针对破坏力极强的勒索病毒，在正常防御手段的基础上，从静态防御和动态防御两个维度专门定制了勒索软件的围猎矩阵，覆盖勒索病毒破坏前、破坏中、破坏后全生命周期，静态防御包括勒索病毒专用 AI 模型，增强对勒索病毒的检

测能力；动态防御包括行为狩猎和勒索诱捕，行为狩猎捕捉勒索病毒删除磁盘卷影、关闭自动修复、删除备份编录等常见危险行为，勒索诱捕对勒索病毒操作诱饵文件的可疑行为进行捕捉。

3.5.4. 内置下一代人工智能引擎 Protoss™

Protoss™人工智能引擎将人工智能、算法和机器学习应用于恶意代码的预测、鉴定和阻止，引擎全自动化完成样本的格式精准识别、文件脱壳解码、文件深度解析、特征提取、特征向量化和人工智能模型的训练和预测。



Protoss™人工智能引擎相比传统引擎具有更快、更强、更轻的特点，在线和离线情况均能够高效检测各类已知和未知威胁。人工智能引擎的研发需要依赖于海量恶意样本的积累、高质量训练样本筛选、长期积累的恶意软件特征、机器学习算法的应用、跨平台工程实现，是高技术难度、高开发量、高维护量的工作，充分体现防病毒厂商的综合实力。Protoss™人工智能引擎代表了国产人工智能杀毒引擎的顶尖水平，具有以下特点：

- 产品级 AI 引擎，部署终端规模达到数百万级；
- 引擎具有高检测率、低误报率、强对抗性的特点，尤其对于未知样本具有很好的泛化检测能力；
- 扫描速度快，充分发挥机器学习算法在多核利用、并行计算方面的优势，在多核环境下最高能够达到传统引擎的数倍扫描速度；
- 支持检测类型覆盖面最广，支持 PE/OFFICE/PDF/ELF 多种格式；
- 实现人工智能引擎恶意代码检测多分类，能够区分出 Virus（病毒）、Trojan（木马）、Ransom（勒索病毒）、RiskTool（风险工具）、Rootkit

（内核木马）、Backdoor（后门）、Exploit（溢出）、Worm（蠕虫）、Hoax（广告）、Unsafe（其它）

- 全平台支持，支持 Windows、Linux、国产操作系统各类平台，支持 X86、ARM、loongarch64、MIPS、Alpha 等多种硬件架构。

3.5.5. 强大的持续采集和检测能力

基于终端强大的信息采集能力（内核态采集，覆盖 Windows 和 Linux 终端行为 20 大类 60 多个子项），依托终端安全大数据平台，以自定义进程唯一 ID 为主线，对攻击者完整攻击行为所采用的攻击步骤进行关联分析，根据攻击事件发生的时间序列，将该次完整的攻击步骤以图形的形式展现，实现攻击场景的重构。通过攻击场景重构的关联规则以及知识的形式化表述，将庞杂、无序的安全数据流转换为结构化、易于理解的攻击场景，将反映攻击过程和意图的场景图呈现出来，从而发现攻击者的攻击策略和目的，甚至推测下一步可能的攻击行为，以便于管理员做出及时有效的应急响应。

3.5.6. 全面支持信创生态

信息技术应用创新发展是一项国家战略，打造中国自主的 IT 底层生态将是我国信息技术领域具有划时代意义的举措。聚铭终端安全管理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，为国产信创终端网络安全保驾护航。

3.5.7. 支持零信任联动

聚铭终端安全管理系统全面支持与第三方零信任解决方案进行联动，支持对主机环境进行感知和度量，支持将主机环境变更主动推送至安全策略控制，协助安全策略控制完成主机的安全环境核查。主机环境感知的内容包括网络环境风险、

恶意代码风险、漏洞风险、系统安全配置风险、应用环境风险和导致主机故障的健康项。

3.6. 使用环境

- 控制中心兼容硬件平台和操作系统

操作系统	版本	浏览器	硬件平台
	CentOS7.5-7.9	Chrome、火狐、Edge	X86（Intel、AMD、兆芯、海光）
	RedHat7.5-7.9	Chrome、火狐、Edge	X86（Intel、AMD、兆芯、海光）
	统信服务器 1060a	Chrome、火狐、Edge	X86（Intel、AMD、兆芯、海光）
	银河麒麟高级服务器版 V10	Chrome、火狐、Edge	X86（Intel、AMD、兆芯、海光）、ARM（鲲鹏、飞腾）

- 受控主机代理兼容操作系统

操作系统	版本	硬件平台
	桌面 Windows XP（32 位）/Win7/Win8/Win10/Win11 服务器 Windows Server 2003（32 位）/2008/2012/2016/2019/2022	X86
	银河麒麟 10 桌面版、优麒麟 V20.10 桌面版、银河麒麟高级服务器版 V10	X86、ARM、loongarch64、MIPS、Alpha
	中标麒麟 7.0 桌面版、7.0 服务器版	
	统信 V20 桌面版	
	深度 V20 桌面版	

	EulerOS 2.0	
	凝思 6.0.80	
	红旗 V9 桌面版	
	中科方德 V3.1 桌面版	
	Ubuntu 10/12/14/16/18/20/21/22/23	X86
	CentOS 6.0-8.5	X86
	Redhat 6.0-8.8	X86
	Oracle Linux Server 6/7/8	X86
	SUSE 11/12/15	X86
	Opensuse-leap 15.2	X86

- 受控主机代理兼容硬件平台

硬件平台	版本	硬件架构
	Intel	X86
	AMD	X86
	飞腾	ARM
	鲲鹏、麒麟	ARM
	兆芯	X86
	海光	X86
	申威	Alpha

龙芯中科 LOONGSON TECHNOLOGY	龙芯	MIPS 和 LoongArch

4. 产品价值

- 降低企业安全风险

主机作为构建信息化网络的基本组成单元和重要元素，具有部署范围广、使用数量多、承担业务多样、存储重要信息数据等特点，容易成为攻击和窃密的对象。聚铭终端安全管理系统能够有效防止针对主机的已知和未知威胁入侵，帮助用户保障关键业务系统和核心数据安全，降低企业安全风险。

- 提升主机运维效率

聚铭终端安全管理系统将多个功能整合至单一的轻量级代理，轻量级代理支持信创终端和非信创终端，支持物理机和虚拟机，通过单一的管理控制台进行集中管理，支持统一杀毒、统一漏洞修复、统一策略分发、统一桌面管控、统一威胁处置、统一升级，显著降低了主机运维的复杂性。

- 事件溯源快速响应

聚铭终端安全管理系统具备强大的系统监控和数据采集能力，全方位记录主机的各类安全数据，安全事件发生之后，能够通过完整的终端安全数据进行追踪溯源，支持事件响应人员快速检索、识别和控制所有受威胁影响的主机。

- 覆盖全栈终端安全

聚铭终端安全管理系统是全栈终端安全解决方案，防护对象包括终端、服务器、虚拟机、云主机和信创环境各种应用场景，产品功能覆盖网络防病毒、终端检测与响应（EDR）、服务器安全管理系统等产品的核心指标，通过单个产品实现终端安全全场景、全功能、全覆盖，避免终端安全类产品的堆砌。