安恒信息
DAS-security 安全中国

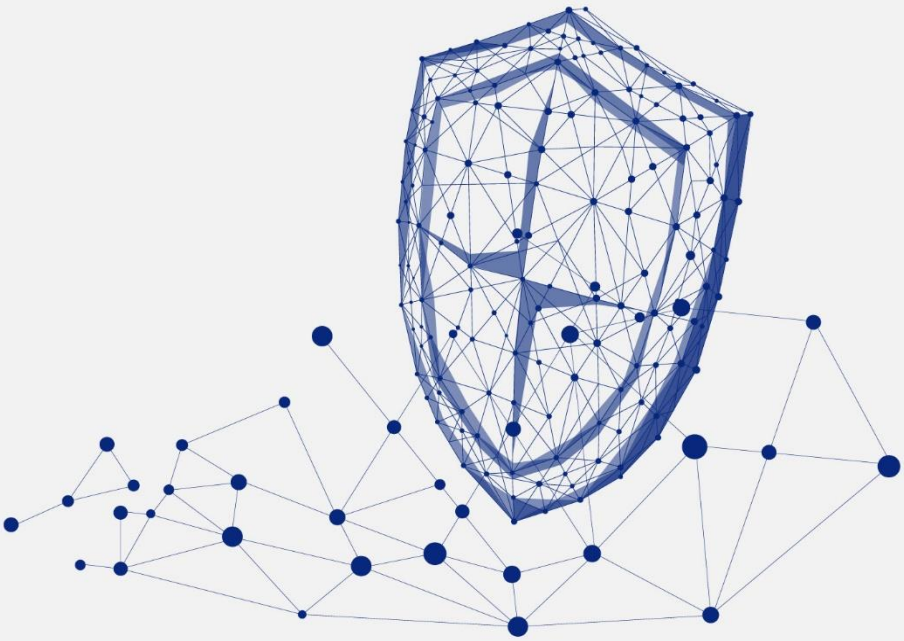
明御®终端安全及防病毒系统（EDR）

V3.0.2

产品白皮书（行业版）

文档版本：01

发布日期：2022-07-25



文档说明

产品名称		明御®终端安全及防病毒系统	
适用平台/版本		V3.0.2	
拟制人	AH4871（物联网+-终端安全）	**评审组**	AH5506（远程技术支持-标准文档）
发布人	AH5888（远程技术支持-标准文档）	**备注**	受控文档

修订记录

日期	修订版本	修改记录	修改人
2022-07-25	01	初次发布	AH4871（物联网+-终端安全）

目 录

前言 I

1 背景信息 1

2 产品概述 2

2.1 产品简介 2

2.2 产品原理 2

3 产品功能 4

3.1 终端管理 4

3.1.1 终端概况 4

3.1.2 病毒防护 6

3.1.3 病毒查杀 7

3.1.4 网马查杀 7

3.1.5 漏洞管理 8

3.1.6 微隔离 8

3.1.7 移动存储 8

3.1.8 分组标签 9

3.1.9 容器安全 9

3.2 高级威胁防御 9

3.2.1 勒索防御 9

3.2.2 挖矿防御 10

3.2.3 渗透追踪 10

3.2.4 情报云脑 10

3.3 策略管理 10

3.3.1 系统防护 11

3.3.2 网络防护 12

3.3.3 渗透追踪 13

3.3.4 网页防篡改 13

3.3.5 Web 应用防护 13

3.3.6 终端体检 15

3.3.7 信任名单 15

3.3.8 桌面管控 15

3.3.9 事件响应 16

3.4 屏幕溯源 17

3.4.1 屏幕隐形水印 17

3.4.2 取证管理 17

3.5 响应处置 18

3.5.1 信息搜索 18
3.5.2 文件推送 18
3.5.3 定期巡检 18
3.5.4 流量画像 18
3.5.5 事件调查 18
3.6 风险评估 18
3.6.1 终端体检 19
3.6.2 基线检查 19
3.7 容器篡改防护及分析 19
3.8 日志管理 19
3.8.1 防护日志 19
3.8.2 操作日志 19
3.8.3 运维日志 20
3.9 日志报表 20
3.9.1 日志 20
3.9.2 报表 20
3.9.3 安全日报 20
3.10 终端可视化 20

3.11 终端全览 20

3.12 角色权限 20

3.13 多级中心 21

4 产品特点 22

4.1 防御已知和未知类型勒索病毒 22

4.2 防御高级威胁全流程攻击 22

4.3 管控全局终端安全态势 22

4.4 全方位的主机防护体系 22

4.5 流量可视化，安全可见 22

4.6 简单配置，离线升级，补丁管理 22

5 部署方案 23

5.1 部署模式 23

5.2 部署拓扑图 23

5.3 部署环境 24

5.3.1 管理平台（中心）部署环境要求 24

5.3.2 客户端部署环境要求 25

5.4 资源占用 25

6 联动方案 26

6.1 AiLPHA **安全分析与管理平台** 26

6.2 **明御**®APT **攻击预警平台** 26

6.3 **明御**®**安全网关** 26

6.4 **明鉴**®**迷网系统** 26

前言

概述

感谢您选择安恒信息的网络安全产品。明御®终端安全及防病毒系统（以下简称“EDR”）是安恒信息在深入分析与研究常见黑客入侵技术的基础上，总结归纳大量的安全漏洞信息和攻击方式后，研制开发的新一代终端安全防护产品。

本手册详细介绍了明御®终端安全及防病毒系统的功能及使用场景等。主要包括背景信息、产品概述、产品功能、产品特点、部署方案以及联动方案。

手册所提供的内容仅具备一般性的指导意义，并不确保涵盖所有型号产品的所有使用场景。因版本升级、设备型号、配置文件不同等原因，手册中所提供的内容与用户使用的实际设备界面可能不一致，请以用户设备界面的实际信息为准，手册中不再针对前述情况造成的差异一一说明。

出于功能介绍及配置示例的需要，手册中可能会使用 IP 地址、网址、域名等。如无特殊说明上述内容均为示意，不指代任何实际意义。

预期读者

本文档主要适用于期望了解明御®终端安全及防病毒系统的读者，包括服务工程师、系统管理员、网络管理员等。本文假设读者对以下领域的知识有一定了解：

- TCP/IP、SNMP 等基础网络通讯协议。
- 终端防护类产品的基本原理。
- 网络安全技术相关知识，包括常用攻击和防御手段。

获得帮助

使用过程中如遇任何问题，请致电服务热线 400-6059-110。

请访问安恒社区 https://bbs.dbappsecurity.com.cn 获取更多文档。

联系信息

地址：浙江省杭州市滨江区西兴街道联慧街 188 号安恒大厦

邮编：310051

电话：0571-88380999

传真：0571-28863666

官网：http://www.dbappsecurity.com.cn

邮箱：400-doc@dbappsecurity.com.cn

1 背景信息

随着互联网的飞速发展，用户在体验互联网带来的无限共享资源的同时，网络威胁也随之而来，病毒感染、木马入侵、黑客攻击等威胁事件时时刻刻都在进行着。

安全行业在经历了大量的网络层工作之后发现，HTTPS、HTTP/2.0 层出不穷的漏洞，已经让网络安全解决方案进入一个进退维谷的状态：无法有效防止终端上的漏洞、无法对终端内部更详细的信息进行分析、有时候检测分析出问题却没办法进行处置。这些困难让我们认识到，终端才是真相之源和控制之本，要真正解决网络安全问题，必须直面困难、必须从实现终端安全开始。

站在防御角度来说，安全防护永远是投入不足的，所以我们必须识别安全的主战场。表面上我们都在解决设备安全的相关问题，如服务器安全、终端设备安全及网络设备安全等等。安全的实质问题并不是设备，人或人为因素才是信息安全问题的根源所在。但人的力量是不能直接作用于信息系统，人与信息系统进行交互，必须要借助载体，这就是人机界面，而人机界面实质上就是终端。

一个安全事件，无论在网络中经过多少环节，用了多少高级技术，其最终目的都是为了完成某些未经授权的工作。比如窃取数据、破坏系统、潜伏以备后续使用等。而这些动作的完成，必须通过某个终端才能完成。正是因为终端是大多数安全事件的目标和发生地，因此终端成为了安全的主战场。

明御®终端安全及防病毒系统正是为解决终端安全而生。

2 产品概述

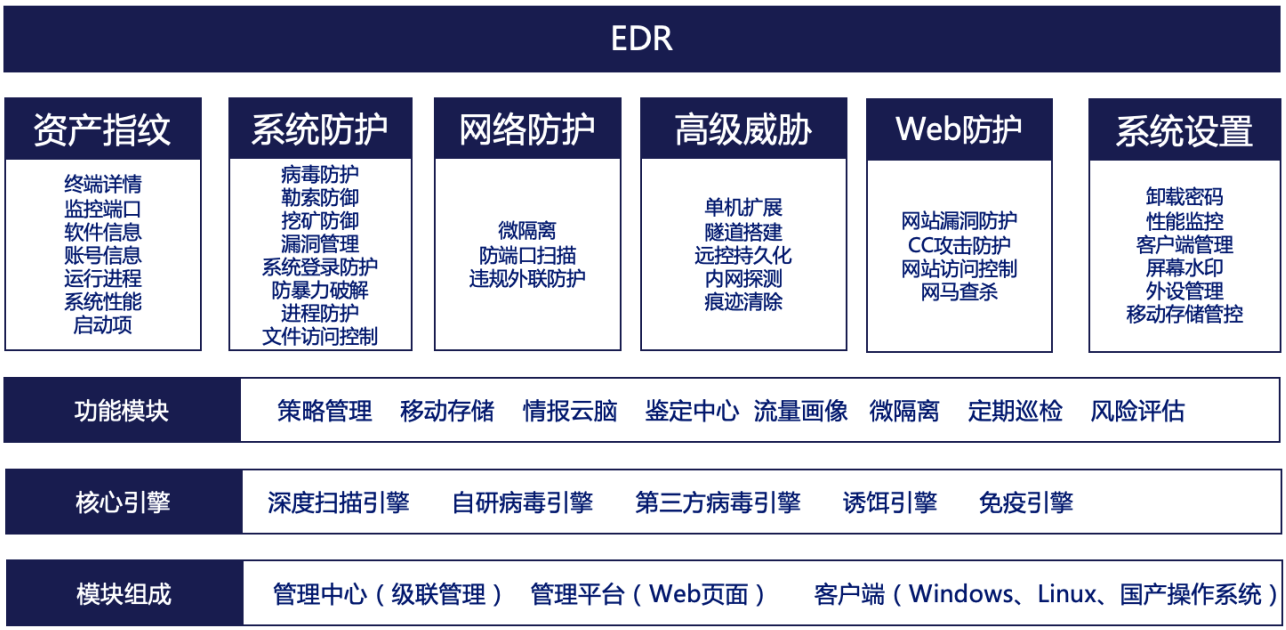
2.1 产品简介

EDR 是一款集成了丰富的系统加固与防护、网络加固与防护等功能的主机安全产品。具有以下特点：

- 具有业界独有的高级威胁防护模块，专门应对攻防对抗场景。具有领先的多个反病毒引擎，配合主动防御技术能够第一时间阻断恶意代码的运行。
- EDR 通过自主研发的专利级文件诱饵引擎，有着业界领先的不依赖反病毒引擎的勒索专防专杀能力，并通过内核级东西向流量隔离技术，实现网络隔离与防护。同时还拥有补丁修复、外设管控、文件审计、违规外联检测与阻断等主机安全能力。

目前产品广泛应用在服务器、桌面 PC、虚拟机、工控系统、容器安全、攻防对抗等各个场景。

EDR 产品功能具体如下图所示。

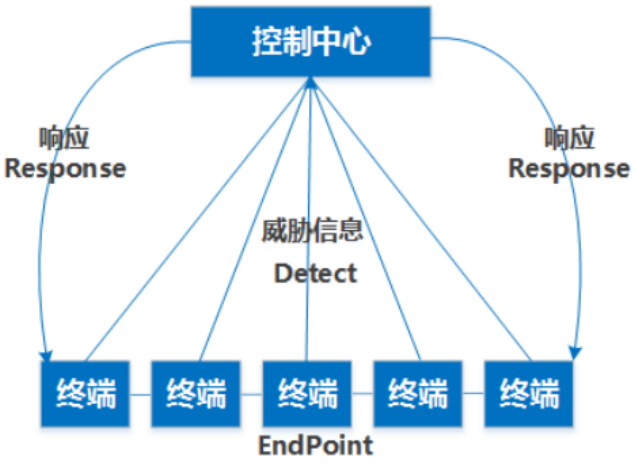


2.2 产品原理

EDR 由管理控制中心和客户端组成。

- 管理控制中心部署在独立提供的 Linux 系统主机上，主要功能为把所有客户端信息集中于一体，便于集中监管和配置安全策略，聚合客户端情报信息进行后续的响应以及处置。管理控制中心采用 B/S 架构，安装完成后，用户可以在任意与管理控制中心网络可达的计算机上访问管理控制中心的 Web 管理平台，对终端进行管控。

- 客户端软件是一个独立的本地可执行程序，安装在需要被管控的主机上，完成管理员通过管理控制中心下发的任务和策略。



3 产品功能

3.1 终端管理

3.1.1 终端概况

◆ **终端详情**

对终端进行详细信息展示，包括网络信息、环境信息及其他信息。可进行远程关机、远程重启、IP/MAC 绑定（Windows）、修改远程管理端口等操作。

◆ **主机发现**

可建立扫描任务，通过管理平台或者任意已部署客户端的主机扫描指定网段，使用 UDP、TCP、主机名称发现的方式发现网段中存在的主机信息。

◆ **IP/MAC 绑定**

- 支持 IP/MAC 绑定操作，能够覆盖 IP 地址、子网掩码、默认网关、DNS 设置的绑定。当检测到绑定的信息被修改，将会自动恢复为原始信息，并在运维日志进行告警。
- 若原 IP 配置是 DHCP 方式，设置绑定后将变为静态 IP 的方式。

◆ **修改远程管理端口**

对终端进行修改远程管理端口操作，修改默认的管理端口可提升系统安全性。

修改管理端口号后需重启远程服务才能生效，用户可选择是否立即重启远程管理服务。

- 若立即重启，重启过程中会断开已连接的会话。
- 若未选择立即重启，则需要用户自行前往终端进行重启。
- 修改后的端口号会自动加入到系统防火墙放行列表，无需用户自行操作。

◆ **监听端口**

- 显示终端上的端口监听与进程的对应关系。
- 支持的显示属性：监听端口号、网络协议、对应进程、绑定 IP。
- 支持实时刷新获取最新信息。
- 此处显示的信息不包含全量的网络连接信息，仅包含监听信息。

◆ **运行程序**

- 显示终端上的运行进程的列表。

- 支持的显示属性：进程名、进程路径、内存占用、CPU 使用率、启动参数、启动时间、运行用户、父进程。
- 可强制终止进程。
- 支持实时刷新获取最新信息。
- 已运行的进程但是无对应的文件，则可能为恶意进程，EDR 会使用不同的颜色进行标记（此特性仅支持 Linux 操作系统）。

◆ **账号信息**

- 显示终端上的账号信息。
- Windows 支持的显示属性：用户名、用户 SID、所属用户组、账户状态、账户类型、账户主目录、是否为域账号。
- Linux 系统支持的显示属性：用户名、UID、GID、账号状态、root 权限、账号登录方式、SUDO 权限、home 目录、Shell、最后登录时间、密码状态、密码修改时间、密码到期时间、密码锁定时间、公钥 KEY。
- 支持实时刷新获取最新信息。

◆ **软件信息**

- 显示终端上已安装的安全软件信息。
- 支持的显示属性：软件名、厂商、版本号、安装目录。
- 支持实时刷新获取最新信息。

◆ **性能监控**

- 以图表形式显示终端上的性能统计数据。
- 支持对 CPU 使用率、内存、网络 IO、磁盘使用率进行监控。
- 策略中可配置性能监控使用率告警值，终端采用轮询采样法计算一个周期内的平均值来判断是否属于性能异常并产生告警日志。

◆ **临时封锁 IP**

- 显示此终端上已临时锁定的 IP 列表。
- 临时封锁 IP 的原因包括：防暴力破解、防端口扫描、防 CC 攻击、屏蔽扫描器都有可能导致临时封锁 IP，具体原因会显示在封锁原因列表中。
- 可解除封锁的 IP，解除封锁后，若继续有违规动作，则依旧会重新被临时锁定。
- 加入到信任区的 IP 地址不会再触发临时锁定。

◆ **启动项**

- 显示 Windows 终端上的启动项信息。

- 支持显示的启动项位置：系统的注册表启动项（包括各类系统插件、Run 项、右键菜单）、应用层服务、驱动、计划任务、WMI 等。
- 操作项支持删除启动项。

◆ **在线统计**

- 显示此终端的在线情况。
- 统计数据包括：终端在线总时长、最近离线时间、离线累计时长、在线累计时长。
- 默认展示最近 7 天的在线统计图表，可更改展示的时间周期。

◆ **资产登记**

- 支持对终端下发登记提醒，登记内容由用户自定义。
- 终端完成登记后，登记信息将展示在终端列表中。

3.1.2 病毒防护

手动进行病毒扫描具有滞后性，EDR 支持病毒实时防护功能，在潜在的风险即将发生之前可介入检测，及时阻断恶意代码的运行。病毒处置时，只清除病毒、不损坏文件，基于“通用脱壳”、“行为沙盒”的纯本地反病毒引擎，无需连接外网。

覆盖的主动防御场景如下。

◆ 代码执行

通常指进程启动、DLL 加载、驱动加载、脚本执行时，会执行恶意代码检查，检出威胁将阻止进程执行并处置病毒。脚本类执行可覆盖无文件病毒的防御，类似 PowerShell、WMI、Rundll32、Register32 等。

◆ 文件改动

当系统中有文件变动时，也会触发恶意代码的检查，可覆盖本机文件改变，浏览器下载文件、聊天软件接收文件。并不是所有的文件变动都会引发恶意代码检查，仅针对潜在的有风险的文件，包括 PE 类格式（EXE、DLL、SYS 等，Linux 的 ELF 格式）、所有的文档类（可能包含宏病毒）、所有的脚本类（Web 动态脚本、PS、PY、BAT、SHELL 等）。

◆ 存储介质连接

U 盘是局域网病毒传播的一种常见手段，EDR 可在 U 盘插入电脑时感知到，并根据设置执行 U 盘病毒检查。

3.1.3 病毒查杀

可从**终端视角**查看所有终端病毒查杀情况，并可对所有终端批量进行病毒扫描（快速扫描/全盘扫描/自定义扫描）、停止扫描及处理病毒操作。

- 支持模板化管理信任名单。
- 支持查看单个终端的病毒查杀页面。
- 支持查杀设置，包括扫描模式（极速模式、低资源占用模式）、多引擎设置（默认引擎、深度扫描引擎）、压缩包查杀设置、处理方式。
- 支持扫描后导出病毒查杀的结果报告。

可从**病毒视角**查看所有病毒威胁情况，并可单独查看病毒影响的终端、文件路径、发现时间、发现方式等信息，对病毒文件进行立即处理或删除记录。

EDR 病毒扫描具有以下功能特点：

- 丰富全面的平台支持：Windows + X86 32 位/64 位、Linux + X86 32 位/64 位、Linux + MIPS 32/64 + 大小字节序、Linux + ARM32 位/64 位。
- 支持多种压缩包、自解压包、复合文档、媒体文件、加密脚本、电子邮件、邮箱文件、可提取文档中嵌入的其它资源，如：宏、脚本、可执行程序等。
- 丰富的脱壳能力及全面的模拟执行能力（反病毒虚拟机）。
- 支持强力查杀功能，可对无法普通隔离的病毒文件进行强制停止进程并隔离、或动态移除到删除队列。
- 支持部分病毒感染文件的修复功能，对于二进制文件可剥离感染部分，保证应用正常使用。自研免疫引擎通过强制访问控制技术免疫 WannaMine1.0/2.0/3.0 等免杀病毒。

3.1.4 网马查杀

可查看所有终端网马查杀情况，并对所有终端批量进行网马扫描、停止扫描、处理网马。

- 支持模板化管理信任名单。
- 支持查看单个终端的网马查杀页面。
- 支持查杀设置，包括扫描模式（极速模式、低资源占用模式）、多引擎设置（默认引擎、深度扫描引擎）、网马引擎、处理方式。
- 支持扫描后导出网马查杀的结果报告。

EDR 网马扫描具有以下功能特点：

- 对网站目录的文件进行全面检测、多重检测技术结合（特征码、模糊 HASH、脚本虚拟机动态检测），对于一句话木马、大马检出率高，误报少。

- 采用先进的多模匹配算法，可极大提升扫描速度。在针对大量文件的情况下，能够在文件不改变的前提下缓存信息，待二次扫描时大幅度提升扫描速度。
- 通过路径配置对 Web 应用目录进行深入检测，对扫描出的风险文件进行立即隔离、添加信任、删除操作。

3.1.5 漏洞管理

可查看所有终端漏洞扫描情况，支持的漏洞类型包括但不限于操作系统漏洞（Windows、Linux 等）、数据库漏洞（MySQL 等）、Web 容器漏洞（Tomcat、Apache、Nginx 等）及其他组件漏洞，支持扫描后的漏洞结果报告导出。同时支持对所有终端批量进行 Windows 漏洞修复。

Windows 漏洞的修复方式是采用微软汇总更新的方案。微软此前一直采用发布单独补丁的形式，随着漏洞数和补丁数逐渐增多，出现了多种问题，如扫描速度慢、测试复杂程度增加等，并且用户是否打补丁，打哪个补丁也都不受控制，有些补丁之间存在依赖关系，缺少其一就会产生错误，由此用户体验也会下降。所以微软在 2016 年宣布，要将此前发布单独补丁的形式调整为发布汇总的补丁。主要分为：“仅安全更新”和“月度汇总”两类，而最新的 Windows 10 系列系统，微软也仅提供汇总方式。

Windows 补丁的“仅安全更新”包含本月所有漏洞的单独补丁，“月度汇总”包含当月的“仅安全更新”和非安全类更新，以及上月的“月度汇总”。因此，用户始终只需一个最新的“月度汇总”补丁，就可以将系统以往的漏洞都修复。一般情况下，最新的月度更新汇总还需要依赖若干个前置更新。做了这个调整之后，微软 2017 年产生的补丁数大大下降，如此，即可避免上述的诸多问题。

3.1.6 微隔离

内核级网络防火墙，由网络驱动技术实现，不依赖系统自身的防火墙。能够对不同的业务之间的流量进行精准识别、针对非法流量可以精准阻断，该功能广泛应用在云数据中心。

操作便捷，直接输入需要关闭的端口或需要屏蔽的恶意 IP，可自动生成隔离规则。

3.1.7 移动存储

对所有终端的移动存储设备进行管控及审计。支持管理员对入网的移动存储介质进行注册，并且对已注册的移动介质进行管理，可以有效防止数据外泄以及移动存储带毒入网的问题。

未进行注册的移动存储设备默认权限按照终端对应的策略模板中“移动存储管控”设置的读写权限执行，已注册的移动存储设备权限优先级高于策略模板。

此功能仅针对有盘符的移动存储设备，例如 U 盘、移动硬盘等。手机、PAD 等虚拟设备不支持管控，仅支持从外设管控中禁用设备。

3.1.8 分组标签

支持对终端进行分组管理，便于对终端进行分类以及进行批量设置。

- PC 组：Windows 7、Windows 8、Windows 10、Windows 11 等操作系统默认划分为 PC 组。
- Windows 服务器组：Windows Server 2003、Windows Server 2008、Windows Server 2012、Windows Server 2016、Windows Server 2019 等操作系统默认划分为 Windows 服务器组。
- Linux 服务器组：Linux 操作系统默认划分为 Linux 服务器组。
- 系统默认组：其他的为系统默认组。

3.1.9 容器安全

用户可对云工作负载保护平台下的容器提供全生命周期安全管控和防护。

- 对容器集群节点中的容器运行状态进行实时监控。
- 支持高危系统调用检测、异常进程检测、文件异常检测、容器环境检测。

3.2 高级威胁防御

3.2.1 勒索防御

勒索病毒防护是系统数据保护的重要一环，也是安恒 EDR 特色与擅长的功能，安恒 EDR 通过全周期（事前、事中、事后）、多维度的防护可对各类已知、未知的勒索软件精准检出与防御，勒索病毒爆发时通过专利级的识别方案，第一时间发现勒索病毒并及时阻断其运行，实时保护用户关键数据。

- 事前体检

  弱点发现、漏洞修复。

- 事中防御

  - 对通用类恶意软件进行主动防御，在进程启动、文件落地、模块加载的时机进行恶意文件扫描，若勒索软件能被杀毒引擎检查到，此时会立即拦截。
  - 勒索诱饵防护引擎

    在磁盘根目录放置诱饵文件，确保调用 Windows API 遍历文件首先遍历到诱饵文件，当对诱饵文件进行操作时，立即告警并结束操作进程。
  - 勒索行为防护引擎

内核驱动级实现，文件过滤驱动监控针对所有文件的操作，当一定时间内，某进程有大量的文件重命名及写入事件触发内置阈值时，未命中内置白名单则告警并结束操作进程。

- 文件保险柜

  内核驱动级实现，用户可自定义关键的数据目录（可配置例外进程），被保护的关键目录变为只读，保障数据安全。

◆ 事后溯源

勒索软件一般执行完毕后会进行自删除操作，当触发 EDR 的针对勒索的防护策略时，会对当前勒索软件进行备份，便于事后确定勒索软件家族、数据恢复。

通过行为识别到的疑似勒索病毒将会备份在系统盘的临时目录中，例如 C:\Windows\Temp\RansomBack。

3.2.2 挖矿防御

挖矿类病毒通常不具备直接危害，但会恶意侵占系统大量资源，对服务器的正常运行造成影响，同时也可能会带来其他恶意代码。EDR 通过匹配挖矿类病毒的常见行为来识别挖矿病毒。

EDR 还能将主机的 DNS 请求域名与威胁情报进行碰撞，能够覆盖挖矿病毒连接矿池域名的场景。

3.2.3 渗透追踪

根据 ATT&CK 理论，对攻防对抗的各个阶段进行防护，实现攻防对抗 360 度防御。同时可通过常见问题，了解渗透追踪的小知识。

3.2.4 情报云脑

情报云脑支持对外联 IP、DNS 解析、可疑文件上传至云端进行鉴定，协助分析其是否存在威胁。

同时提供智能鉴定功能，在用户同意云端鉴定的前提下，上传可疑的外联 IP、DNS 解析、可疑文件至云端进行鉴定，并可快速查看鉴定结果。

3.3 策略管理

策略管理可以查看具体的防护配置，同时支持新增、编辑和删除策略。调整好的策略可以绑定到终端上，终端也可以随意切换策略。对于已经绑定终端的策略，后续只需要更新策略，已经绑定的终端将会同步更新策略。

系统内置三个模板，分别为通用模板、业务模板和审计模板。这三个模板已基本涵盖日常运营的大部分场景。同时用户可设定默认模板，新增终端将自动添加至默认模板。

3.3.1 系统防护

病毒防护

在文件执行时或进入主机时进行病毒扫描，实时发现病毒。并进行文件落地查杀、新增模块加载、脚本加载、驱动加载时防御。针对感染性病毒以及宏病毒提供修复能力，且支持多引擎防护。

勒索防御

内核级防御引擎，第一时间发现并阻断勒索病毒的加密行为，实时保护用户关键数据。

- 勒索诱饵防护引擎针对勒索病毒遍历文件实施加密的特点，在终端关键目录下放置诱饵文件，当有勒索病毒尝试加密诱饵文件时及时中止进程，阻止勒索病毒的进一步加密和扩散。
- 勒索行为防护引擎通过分析常见的勒索软件样本，总结了样本具有的共性特征，形成引擎行为库。系统 API 级别分析，有效抵御未知勒索病毒。
- 文件保险柜添加访问控制策略，对重要文件进行访问权限控制，仅允许配置的例外进程操作，避免被勒索病毒破坏。

挖矿防御

反挖矿引擎通过分析程序行为及其它指标实时发现恶意挖矿程序，能实时发现未知恶意挖矿程序。

漏洞管理

采用漏洞库的方式进行检测，可精确快速地根据不同的操作系统定位到未安装的补丁，依靠管理平台的推送功能，可将漏洞库文件推送到终端上安装最新补丁，免受黑客攻击。

每个补丁均经过人工验证，并且在补丁的依赖关系上增加了重启验证机制，保证了补丁安装的稳定性。即使终端无法连接互联网，也可依赖管理平台的离线补丁下载器将补丁文件导入到管理平台，后续终端即可正常下载安装补丁。

漏洞管理功能可对主机系统进行全面漏洞扫描，并对漏洞补丁进行一键修复或单个修复。补丁修复存在一定风险，需测试后再进行修复，以免对正常业务造成影响。

根据中心和客户端主机是否可访问互联网的不同情况，漏洞补丁的获取方式如下。

联网情况	获取方式
只有中心可访问互联网	通过 admin 账户登录中心，在中心上收集补丁后推送给客户端主机进行修复。
只有客户端可访问互联网	中心已下载过的补丁由中心推送给客户端主机进行修复；中心未下载过的由客户端主机下载进行修复。

联网情况	获取方式
中心和客户端都不可访问互联网	通过 admin 账户登录中心，离线上传补丁后，中心推送给客户端主机进行修复。
中心和客户端都可访问互联网	中心已下载过的补丁由中心推送给客户端主机进行修复，中心未下载过的由客户端主机下载进行修复；或选择中心去收集补丁后推送给客户端主机进行修复。

系统登录防护

使用操作系统本身公开的安全登录插件机制实现系统登录防护功能，相较于传统的读取系统日志判断的方法，插件防护不会遗漏掉任何登录数据，更加安全。

EDR 对系统账户登录进行细粒度的精准访问控制，支持对访问来源（账户、远程 IP 或域名、远程计算机名）、访问时间进行配置，并能实时阻断非法登录。触发登录防护规则后，自动联动添加微隔离规则。

防暴力破解

当某个 IP 在设置的时间周期内登录系统的失败次数达到一定数量时，会将该恶意探测 IP 锁定，防止其进一步试探获取系统登录口令。用户可在终端详情内查看并解除已临时锁定的 IP。

进程防护

使用内核驱动技术，每当有进程启动时从操作系统内核中可以得到通知，获取到包括进程路径等一系列上下文信息后，可以根据用户需求设置为黑名单直接拒绝或白名单直接放行。支持仅记录模式、阻断并记录模式。

文件访问监控

使用系统文件过滤驱动技术，可细粒度审计文件创建、删除、写入和重命名等操作。

反弹 Shell

采用进程调用命令行分析、Socket 重定向检测等机制发现反弹 Shell。

3.3.2 网络防护

防端口扫描

在网络驱动中检查入站到本机的数据包，当某个 IP 在设置的时间周期内连接本地的不重复的端口数量达到一定次数时，可将该恶意探测 IP 锁定，防止其进一步获取终端敏感信息。

用户可以查看并解除已临时锁定的 IP 清单。

流量画像

流量画像通过绘制内网全景流量图，展示了内网主机间的通信关系和内网主机对外通信情况。并可在发现威胁后对主机间通信进行一键阻断。详情可参考流量画像。

网络分域隔离

可根据业务需要，将网络划分为多个较小的安全信任域并将主机放入。用户可在信任域内部实施较松的安全策略，而信任域边界实施较为严格的监控与访问控制。终端切换到特定网络域后，将无法访问其他所有自定义网络域地址。

3.3.3 渗透追踪

单机扩展

针对本机的扩展行为（信息收集、本机提权等）进行监测，防止提权行为和信息泄露。

隧道搭建

识别渗透过程中的隧道代理（内网穿透、端口转发、代理等），可阻断隧道代理搭建行为。

远控持久化

对失陷后主机远控持久化（反弹 Shell、远程控制）行为进行检测，可阻断远控。

内网探测

对内网的恶意攻击行为（哈希传递、漏洞利用、横向移动）进行识别，可阻断恶意探测行为。

痕迹清除

可对渗透的收尾阶段的数据清理行为进行识别和阻断。

3.3.4 网页防篡改

保护文件不被篡改，默认保护所有子目录，通过新增白名单的方式实现对子目录的排除。支持仅记录模式、阻断并记录模式。

3.3.5 Web 应用防护

由使用 Web 容器的第三方安全插件机制实现，可在 Web 后台程序处理请求之前获取到所有的请求上下文信息提前过滤，对恶意请求及时拦截。

支持容器类型丰富：IIS6.0 ~ IIS10.0、Apache2.2 ~ Apache2.4、以及任何支持 Servlet 过滤模型的 Java 类容

器（Tomcat、WebLogic、JBoss、Jetty 等）。IIS 系列可支持插件的动态安装及卸载，不需要重启 Web 容器。

网站漏洞防护

网站漏洞防护具有以下四大功能：

- 针对常见的 SQL 注入、XSS 跨站攻击进行防护。
- 可检测到各种主流扫描器行为，根据设置屏蔽对本站的扫描。
- 可防护低版本 Web 容器的文件名解析漏洞、畸形文件漏洞等。
- 针对集中爆发的 Web 应用程序漏洞（Struts 系列漏洞等）可及时更新策略达到免疫效果，自定义的网站漏洞防护，可对页面请求的所有字段进行过滤，并能支持对自定义的请求字段（用户业务自定义字段）进行过滤。

CC 攻击防护

以自研 Web 容器安全插件采集的数据为依据，智能检测并防御 CC 攻击行为。同时与微隔离模块达成联动响应，从内核网络驱动中直接丢弃攻击者的数据包，以保证网站的正常服务能力。

CC 攻击防护等级详细说明如下表所示。

级别	说明
低	最简单验证策略，当单个 IP 在规定的时间周期内访问次数达到设置阈值时，将自动锁定一段时间。低级别兼容性最好。 浏览器行为验证说明：当达到规定的访问次数时，如果开启了此选项并且用户是通过浏览器来访问的网站，则说明是正常用户，不会将此 IP 拉黑。该选项可以将正常用户和攻击工具、爬虫类程序进行区分。
中	对于低级别无法防御的情况，可以尝试开启此安全级别。该级别可以智能判断访客的真实性，并且无需访客参与验证，使用了 Cookie、JS 脚本混合验证方式。
高	对于长期处于被攻击状态的网站，建议开启高级别模式，高级别模式安全性最高，会在访客首次访问时通过输入一个随机的验证码来确认（图片方式验证码，具有对抗图片识别工具的干扰色），通过验证后进行浏览时无需再次输入验证码。

网站访问控制

- 支持对一个 IP 或 IP 范围进行 Web 应用层面的细粒度访问控制。网站访问控制的策略优先级高于网站漏洞防护策略。
- 支持对网站的 URL 进行配置，也可通过直接设置域名达到全站放行。

3.3.6 终端体检

终端感知设置

自定义终端环境感知频率及评分上限，可对病毒风险感知，漏洞风险感知，应用合规感知，网络风险感知和终端健康感知进行扣分权重设置。

病毒风险感知

针对病毒程序文件风险、系统恶意代码感染风险进行感知。

漏洞风险感知

针对系统漏洞风险、中间件漏洞风险进行感知。

网络风险感知

针对网络变化风险进行感知，可对 IP 地址变化和 DNS 地址变化进行风险等级的设置。

应用合规感知

针对终端上运行的应用、服务、注册表进行感知。

终端健康感知

针对系统整体的健康状态进行感知。

3.3.7 信任名单

- 信任名单添加文件路径或 MD5 值时，可针对护网高级威胁、病毒防护、病毒扫描、网马扫描、勒索防护进行放行。
- 信任名单添加 IP 时，可针对防暴力破解、防端口扫描、Web 应用防护进行放行。

3.3.8 桌面管控

卸载密码

支持设置客户端卸载密码，防止客户端被意外卸载。已设置的密码支持反向显示。

系统性能监控

对终端的 CPU、内存、磁盘及网络入站、出站流量进行监控，并在达到用户配置的阈值时及时发出告警，防止系统资源耗尽。

客户端管理

显示桌面图标，并设置客户端随系统自启动。

屏幕水印

当用户需要对通过屏幕拍照泄密数据的行为进行溯源时，可使用屏幕水印功能。

屏幕水印设置说明如下表所示。

水印设置	说明
水印内容	终端名称、IP、MAC、登录用户、系统时间、自定义内容。
内容颜色	终端水印的文字颜色。
字体大小	终端水印的字体大小。
文字倾斜角度	终端水印的文字的倾斜角度。
行间距	单个水印之间的文字距离。
块间距	两个水印之间的文字距离。

外设管控

- 按设备类型管控
  包括光驱、软驱、打印机、调制解调器、红外设备、蓝牙设备、摄像头、鼠标、键盘、手机/数码等设备。
- 按接口类型管控
  包括 USB 接口、串口/并口、1394 控制器、PCMCIA 等接口。

移动存储管控

用户可对移动存储设备的默认读写权限及使用审计进行权限设置。

违规外联

在网络驱动中检查本机的出站数据包，由内核中的快速匹配算法支持，即使在有大量规则的情况下，对网络性能的影响也可忽略不计。支持放行、关机模式与断网模式。

开关机审计

通过系统日志、系统事件监控实现，支持全时段、指定时间段对终端的开关机事件进行审计。

3.3.9 事件响应

支持用户设置终端响应动作。

文件变更

- 告警（是否产生告警日志）。
- 删除文件（删除此文件）。

进程变更

- 告警（是否产生告警日志）。
- 删除文件（删除此进程对应的文件）。
- 结束进程（结束此进程）。
- 网络隔离（阻止终端的所有网络连接）。

网络连接

- 告警（是否产生告警日志）。
- 网络隔离（阻止终端的所有网络连接）。

账号变更

- 告警（是否产生告警日志）。
- 账号登出（登出此账号）。
- 账号删除（删除此账号）。
- 账号禁用（禁用此账号）。
- 结束进程（结束此账号运行的进程）。

3.4 屏幕溯源

3.4.1 屏幕隐形水印

对终端设备的屏幕隐形水印进行配置，包括水印强度等，包含不同分辨率和场景下的不同强度的水印效果配置。

3.4.2 取证管理

取证模块通过解析屏幕图片，对图片中水印信息进行提取和还原，获取终端设备信息、图片生成时间和对应的用户信息等的。支持包括屏幕拍照图、屏幕截图和屏幕录屏视频等文件格式，每次取证保存取证记录，支持在线生成取证报告，报告内容包括图片素材信息、溯源标识、时间戳等信息，并支持 PDF 等通用文档格式导出取证报告。

3.5 响应处置

3.5.1 信息搜索

用户可采集所有终端的监听端口、运行程序、账户信息、软件信息及启动项信息，并支持对信息进行下载。

3.5.2 文件推送

当用户需要下发文件、安装应用程序到终端上或者远程执行命令时，可以使用文件推送工具。

3.5.3 定期巡检

设置需要定期批量执行的检测任务，内容包括任务名称、执行巡检的内容、要巡检的终端、执行周期和巡检备注。

3.5.4 流量画像

流量画像通过绘制内网全景流量图展示内网主机间的通信关系和内网主机对外通信情况，发现威胁后可对主机间通信进行一键阻断。

流量画像功能首页对全景流量图进行展示，用户可根据 Windows 服务器、Linux 服务器、PC 三类主机和端口、时间进行过滤查看；通过自定义模板，可根据终端分组、终端标签、终端名称、终端 IP（条件之间的关系为且/或）进行过滤查看，无遗漏查看内网主机通信情况。

- 对于单个主机，可查看其通信关系图和通信关系列表。列表信息包括通信方向时间、IP、端口、协议、时间、次数，大量通信信息可以进行过滤查看。
- 对于通信路径，也可查看其通信关系列表，列表信息包括时间、IP、端口、协议、时间、次数，便于用户分析威胁产生时间，追溯攻击源。

3.5.5 事件调查

用户可通过配置数据采集，查询到所有终端的文件、运程、网络连接、DNS 查询、端口监听、账户、启动项及计划任务的相关信息。

3.6 风险评估

3.6.1 终端体检

可建立扫描任务，通过管理平台或者任意已部署客户端的主机扫描指定网段，发现网段中存在的主机信息。

终端评估

对终端的整体风险进行评估，并给出风险数值，满分为 100 分。

勒索评估

检查系统中的弱口令、系统漏洞等易被勒索的风险项，并给出感染勒索病毒的概率。

弱口令评估

检查系统中存在的弱口令账号，并进行展示。

3.6.2 基线检查

支持操作系统层面的等保基线检查，用户可选择等保基线策略和执行时间，对单个终端或批量终端执行检查任务。支持查看单个任务的基线检查结果，查看影响的终端名称，终端 IP 并进行操作。

3.7 容器篡改防护及分析

支持对云工作负载保护平台下的容器通过规则对目录进行保护，并且可快捷查看到规则名称、保护镜像名、保护容器目录、允许改写进程、备注等信息。

支持对云工作负载保护平台下的容器进行篡改数据的相关分析，如网站篡改分析、篡改源分析等。并支持导出和生成报表（导出报表格式支持 PDF、HTML、DOC）。

3.8 日志管理

3.8.1 防护日志

从容器视角记录防护日志，包括渗透追踪、系统防护、网络防护等日志类型。并支持导出和根据关键字进行搜索查询。

3.8.2 操作日志

可查看用户登录日志、修改密码日志、策略管理日志、分组标签日志、移动存储日志、告警配置日志、资产解绑日志、启用/停止防护日志及短信发送日志。

支持导出日志信息和根据关键字进行搜索查询。

3.8.3 运维日志

可查看资产日志（资产上线、资产离线、资产安装、资产卸载、资产升级、开关机日志、账号创建日志）、性能监控日志（CPU 监控、内存监控、网络 IO 监控、磁盘监控、熔断监控）、外设管控日志（外设使用审计、文件拷贝审计）及运维操作日志（文件推送、病毒扫描、病毒处置、网马扫描、网马处置、漏洞扫描、漏洞修复、弱口令扫描、IP/MAC 绑定）。

支持导出日志信息和根据关键字进行搜索查询。

3.9 日志报表

3.9.1 日志

从攻防视角记录平台日志，包括防护日志、操作日志、运维日志等日志类型。并支持分类和根据关键字进行搜索查询。

3.9.2 报表

对事情趋势和病毒以及风险终端进行图表展示，并支持导出多种格式报表。

3.9.3 安全日报

设置需要定期发送的安全日报，内容包括资产分布风险、漏洞趋势、攻击趋势、安全告警和软件漏洞列表。

3.10 终端可视化

在管理平台界面顶部新增可视化大屏入口，可查看终端管控可视化大屏、安全态势可视化大屏，滚动展示终端部署、防护、资源、告警等信息。

3.11 终端全览

可通过终端全览查看终端的全局信息，并根据终端前往指定的租户进行管理。

3.12 角色权限

支持自定义用户及自定义角色功能，可以根据实际的业务需求，灵活的自定义创建角色并且赋予角色自定义功能权限。租户可以创建不同角色的用户，实现多个用户对终端的共同管理，让终端管理更精细化、更安全可控。

3.13 多级中心

用于下级中心连接上级中心，并且上级中心可以查看所有下级中心的部署情况以及风险数据。

中级中心的目的是为了减少主服务器的业务压力、减轻带宽占用、降低管理成本并解决分支机构、异地联动、多部门协同的难题。

4 产品特点

4.1 防御已知和未知类型勒索病毒

EDR 不仅可以阻止已知勒索病毒的执行，而且在面对传统杀毒软件束手无策的未知类型勒索病毒时，EDR 会采用诱饵引擎，在未知类型勒索病毒试图加密时发现并阻断其加密行为，有效守护主机安全。

4.2 防御高级威胁全流程攻击

EDR 根据 ATT&CK 理论，对攻防对抗的各个阶段进行防护，包括单机扩展、隧道搭建、内网探测、远控持久化、痕迹清除。不仅可以做到威胁攻击审计，而且还可以防止黑客进行渗透攻击，实现攻防对抗 360 度防御。

4.3 管控全局终端安全态势

服务器、PC 和虚拟机等终端安装了客户端软件后，上传终端指纹、病毒木马、高危漏洞、违规外联及安全配置等威胁信息到管理控制中心。用户在管理控制中心可以查看所有安装了客户端软件的主机及安全态势，并进行统一任务下发、策略配置。

4.4 全方位的主机防护体系

EDR 不仅包含传统杀毒软件的病毒查杀、漏洞管理、性能监控功能，同时，在系统防护方面还可做到主动防御、系统登录防护、系统进程防护、文件监控，并支持网络防护、Web 应用防护、勒索挖矿防御、外设管理等多种功能。

4.5 流量可视化，安全可见

EDR 通过流量画像的流量全景图，展示内网所有流量和主机间通信关系，梳理通信逻辑，以全局视角对策略进行规划，便于用户第一时间发现威胁，一键清除威胁。

4.6 简单配置，离线升级，补丁管理

EDR 支持用户自主进行安全配置，能够明确、有效地进行主机防护。主程序、病毒库、漏洞库、补丁库、Web 后门库、违规外联黑名单库全部支持离线导入升级包、一键自动升级，并可在专网使用。

5 部署方案

5.1 部署模式

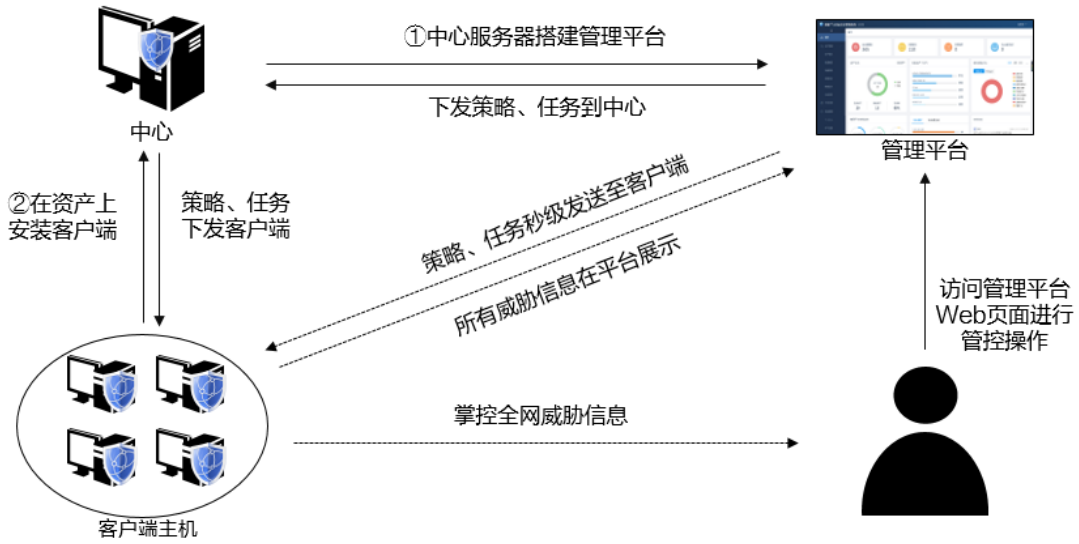
明御®终端安全及防病毒系统是一款集成了系统防护与加固、网络防护与加固等功能的主机安全产品，可广泛应用在服务器、桌面 PC、虚拟机、工控系统、国产操作系统、容器安全等场景。

EDR 产品以软件发货为主，支持 1/N 单中心（管理平台）部署模式和 N/N 多中心（管理平台）级联部署模式，详细见下表。

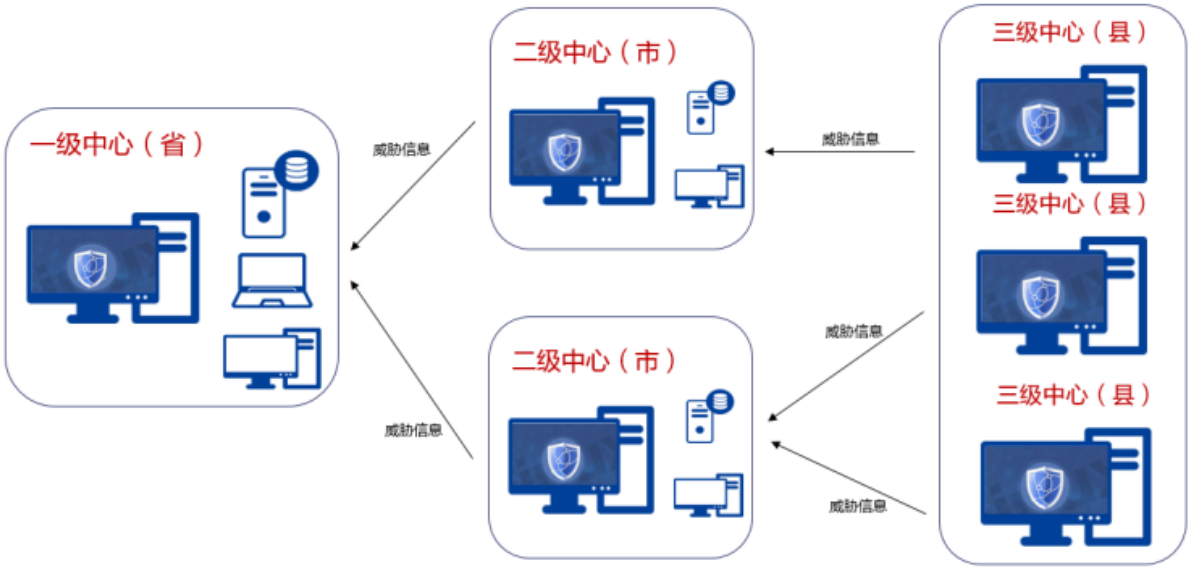
部署方案	适用场景	部署特点
1/N 单中心部署	普通应用场景	◆ 一个中心，N 个代理。 ◆ B/S 部署架构，通过控制中心就可以实现所有主机终端的统一管理。
N/N 多中心级联部署	◆ 省、市、县多级联动场景 ◆ 总部、分支机构联动场景 ◆ 其他复杂网络环境场景	◆ N 个中心，分层级联部署。 ◆ 单个中心部署架构跟 1/N 模式相同。 ◆ 支持多级、分层控制和联动。

5.2 部署拓扑图

◆ 对于 1/N 单中心部署，部署拓扑如下图所示。



◆ 对于 N/N 多中心级联部署，部署拓扑如下图所示。



5.3 部署环境

管理控制中心安装环境需要在“干净的（未安装其他软件的）”操作系统（包括 Windows 系统和 Linux 系统）下部署，否则可能由于组件冲突导致产品运行异常。

5.3.1 管理平台（中心）部署环境要求

当前支持在 Linux 系统环境下部署管理平台（中心）。

Linux 版管理平台部署环境支持 X86 架构、ARM 架构及 MIPS 架构，安装中需要使用 **root** 账号。

- **X86 架构：**支持 **64** 位 **CentOS 7.X** 操作系统及兆芯+中标麒麟 V7.0、V10 操作系统。
- **ARM 架构：**支持鲲鹏+统信 UOSV20 操作系统。
- **MIPS 架构：**支持龙芯+统信 UOSV20 操作系统。

系统所需要的 CPU、内存和磁盘控件要求根据管理终端的数量有所区别，详细请参考下表。

管理终端数量	CPU 核数	内存	可用磁盘空间
1000	不低于 4 核	不低于 8GB（服务器无其他业务运行，闲置运行内存不低于 6GB）	不低于 500GB
2000	不低于 8 核	不低于 16GB	不低于 700GB
5000	不低于 16 核	不低于 32GB	不低于 1TB
10000	不低于 32 核	不低于 64GB	不低于 1.5TB
20000	不低于 64 核	不低于 128GB	不低于 2TB

5.3.2 客户端部署环境要求

EDR 客户端支持在当前绝大部分主流的 PC 和服务器上进行安装部署。

许可类型	客户端系统	支持情况
PC	Windows	支持 **Windows XP(SP3)/Vista/Windows 7/ Windows 8/Windows 8.1/ Windows 10、 Windows 11** 等操作系统。
Server	Windows	支持 **Windows Server 2003(SP2)/Windows Server 2008/Windows Server 2008R2/Windows Server 2012/Windows Server 2012R2/Windows Server 2016/Windows Server 2019/Windows Server 2022** 等操作系统。
	Linux	◆ 支持 **Centos5.0+、Redhat5.0+、Suse11+、Ubuntu14+**等主流操作系统。 ◆ 国产系统支持中标麒麟、银河麒麟、统信 UOS 操作系统。 ◆ 使用 **uname -a** 命令检查 CentOS 内核版本，支持 V2.6.18 及以上版本内核。详细内核版本支持信息可联系安恒信息工程师获取。

5.4 资源占用

正常情况下 EDR 客户端软件的资源占用情况如下表所示。

类型	资源占用量
配置	Win7_x64+2core+2G
进程	Agentservice.exe
CPU（平均值）	1% ~ 5%
内存（MB）	50MB 左右

6 联动方案

EDR 可以与安恒信息的多个安全产品进行联动，提高用户网络的安全防御能力。

6.1 AiLPHA 安全分析与管理平台

通过 EDR 的终端信息采集能力和终端防护能力，将 30 多个维度的模型数据提供至 AiLPHA 安全分析与管理平台进行高级威胁分析。且最终由 EDR 进行处置，形成高级威胁分析及处置解决方案。

6.2 明御®APT 攻击预警平台

在常见黑客入侵技术的基础上，推出边界到端的“检测+防御”体系，通过明御®APT 攻击预警平台对边界的已知和未知威胁检测及定位，EDR 对终端受攻击主机有效防御，形成联合防御方案。

6.3 明御®安全网关

通过集合安恒信息的云端防护能力、明御®安全网关（DAS-Gateway）的管道防护能力以及 EDR 的终端防护能力，打造“云管端”的立体化安全解决方案。

6.4 明鉴®迷网系统

支持与明鉴®迷网系统联动，从而实现自动流量代理、自动蜜饵布防、主机层面的攻击 IP 拦截等能力。