杰思猎鹰主机安全响应系统 V5.0

产品彩页

北京杰思安全科技有限公司

目 录

杰思猎鹰主机安全响应系统 V5.0

1. 主机安全新形势

云计算、大数据、泛在互联、端点智能化移动化的浪潮正在席卷全球，信息科技为全球各行各业注入了绿色高效发展的新动力，网络和应用的开放、复杂、变化成为新常态。

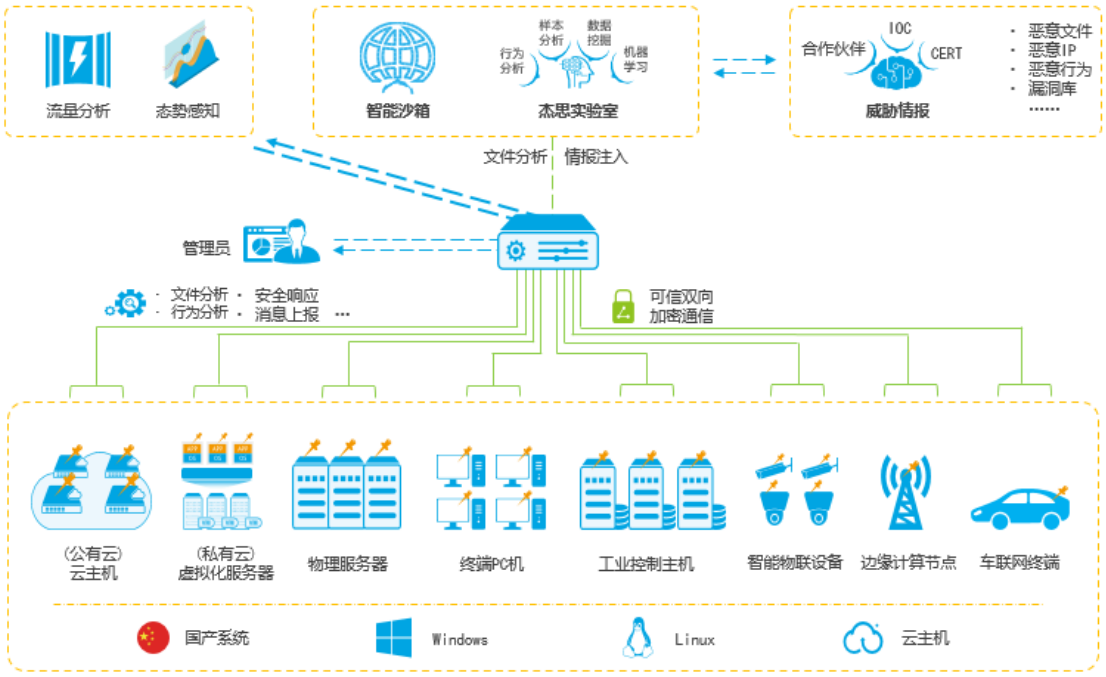
今天的政企数据安全至关重要，安全的保护对象从传统 IT 设施扩展到更广泛的关键信息基础设施。开放、复杂、变化的网络和应用导致在信息安全角度更易被攻击、失陷后扩散更快，更要命的是："谁进来了不知道、是敌是友不知道、干了什么不知道"。

关口前移，以主机安全为重中之重的泛终端（服务器、云主机、PC 机、工控主机、移动智能终端、物联网终端、车联网终端等）成为安全大势所趋，尤以 EDR 端点检测与响应、自适应安全架构、CWPP 云工作负载保护平台、可信计算、工控安全、物联网安全等细分领域最为热门。

2. 基于操作系统的检测与防护

2.1. 产品简介

杰思猎鹰主机安全响应系统 V5.0，为用户提供基于操作系统的威胁检测和防护。凭借 EDR、CWPP、自适应微隔离等前沿安全技术，提升用户抵御未知威胁（包括勒索软件、0day 漏洞、无文件攻击、APT 攻击、免杀木马等）的能力，增强对全网主机内部安全状况的掌控能力，弥补传统安全防护体系不足。经过多年的技术投入与用户场景迭代，已成为新形势下安全建设中不可或缺的安全产品。可广泛部署于安装了 Windows、Linux、国产操作系统的服务器、云主机、PC 机、工控主机、移动智能终端、物联网终端、车联网终端等泛在行业主机，并在政府、运营商、金融、能源、交通、教育、医疗、制造业、互联网等行业得到规模应用。



杰思猎鹰主机安全响应系统 V5.0 部署逻辑图

杰思猎鹰主机安全响应系统由安全探针、管理平台和外围联动三部分组成。

安全探针：

部署在受保护的主机上，进行主机安全信息采集、威胁发现与响应处置。内置微型分析引擎，可实现单点行为、文件的实时分析与响应处置。支持 Windows、Linux 及多个国产操作系统，对计算资源消耗极少。可部署在服务器、云主机、PC 机、工控主机、移动智能终端、物联网终端、车联网终端等不同类型的设备中。

管理平台：

统一管理安全探针，可根据管理规模选择单台集成部署或分布式部署，支持集中式威胁及数据分析、事件汇总可视化展示、安全策略集中管理、程序及特征更新等。

外围联动：

通过智能沙箱和杰思安全实验室进行辅助检测判断。智能沙箱采用云端或私有化部署交付，满足不同场景的使用需求，可提供文件安全性的辅助判断。可与杰思安全实验室或第三方合作伙伴共享威胁情报，可在线或离线更新，包括恶意文件信息、恶意 IP 信息、恶意行为信息、漏洞库信息等内容。

2.2. 产品价值

杰思猎鹰能够帮助安全管理员快速精准地识别风险主机，实时追溯与响应，弥补传统安全防护不足，提升用户抵御网络威胁的能力。

- 扫清网络安全“最后一公里”盲区，帮助用户拿回业务主机安全主动权。

- 与现有网络安全能力互补，并能为态势感知等大数据安全平台提供有效的一手数据。
- 极大的缩短主机威胁的发现到响应处置时间，安全人员可轻松管理数万台主机。

3. 产品技术架构

经过不同场景、复杂环境中的多次部署实践，杰思猎鹰不断提升技术能力，已经形成一套可满足不同行业、不同主机类型、不同数量规模的技术架构体系，为用户提供更好的安全防护效果和产品体验。

杰思猎鹰主机安全响应系统 V5.0 技术架构示意图

为增强产品稳定性和扩展性，更大地提升性能、满足百万级主机同时接管，杰思猎鹰采用了大数据平台层级架构设计。每个层级计算资源独立，可依据管理规模横向扩展。

安全探针检测与响应，为管理平台数据处理提供主机安全原始数据，并提供文件和行为分析及实时响应。在安全探针上做第一层安全分析，保证探针在离线时也能提供正常的安全防护，可保障防护实时性。

管理平台对原始数据进行分布式接入、元数据存储及数据分析深度处理。为主机资产管理、安全风险检测、安全基线管理、主机微隔离、网络威胁防护、入侵行为检测、安全事件溯源、安全监控等安全应用提供支撑。

通过标准的 SSO 接口，可与第三方安全产品做数据共享以及联动响应，也可与云端智能沙箱、杰思安全实验室实时通信，持续更新最新威胁情报。同时，提供 B/S 可视化交互管理及大屏展示。

4. 产品特点

4.1. 看清主机内行为

清晰直观显示所有主机内部系统变化，看清用户业务在操作系统运行时面临的安全风险。

4.2. 入侵威胁溯源

实时对黑客入侵客户业务主机过程进行“行为画像”，图形化展示威胁事件来源、传播途径、影响主机数量范围等，并统一防御和处置。

4.3. 轻量设计，超强适配

软件占用主机资源极低，安装简单快速，在操作系统界面上无弹窗打扰，全面支持 Windows、Linux 以及多个国产操作系统。

4.4. 未知网络威胁检测防护

对于业务主机上传统杀毒软件库内没有的未知威胁，通过端点检测与响应核心技术，实时检测与分析入侵点和感染途径，并全网排查感染主机，及时处置和实时防护。

4.5. 主机安全集中管理

提供所有业务主机内的系统操作，业务更新变化，人员使用情况，专用主机、业务服务器、云主机安全管理“一把抓”，扫清主机安全管理分治造成的监控真空，提升安全管理和应急响应效率。

5. 产品功能

- 资产识别

基于主机安全视角，帮助用户快速梳理和清点主机资产信息，从主机硬件资产、系统资产到上层软件资产、账户资产，自动构建全面的资产安全视图。资产信息清晰可见，让用户对全网资产情况了如指掌；自动发现、自动分组、自动记录变更信息等功能，智能快速构建自适应主机安全防护边界，实时掌控变化。

- 基线检查

基于等保 2.0 以及工信部[YD/T 2701-2014]标准要求内容，制定涵盖 Windows、Linux 及多个国产操作系统的安全基线检查，包括防火墙、账号口令、日志、组策略配置等，内置多个行业和场景检查模版，提供基线修改指导，科学提高系统安全短板。

- AI 风险检测

基于 EDR 理念进行主机多锚点风险检测，从行为合规检测、系统漏洞检测、注册表异常检测、关键配置检测、风险文件检测、账户风险检测等进行全局立体风险透视。同时，结合自适应资产安全视图，呈现可视化的主机风险全貌，帮助用户在庞大网络内对风险主机进行秒级定位。

- 智能响应

融入机器自学习技术，贴合用户业务场景，不断进化用户侧行为检测与响应模型，响应精准度＞99%。提供多种响应防护模式，结合近百种风险分类，可形成数十万个响应方案组合，提供不同业务场景下更理想的响应方式，为每个用户提供私人订制的响应方案。

- 自适应微隔离

基于现代混合数据中心架构，提供端点和业务视角的双向网络微隔离，帮助用户梳理构建业务安全边界，解决云数据中心东西向流量防护难题。可视化访问模型帮助用户梳理业务访问，采用自适应安全域与策略管理，弹性扩展安全防护，适应云工作负载安全（CWS）解决方案。

- 态势分析

自动化资产与风险感知，利用庞大的端点安全数据支撑，精准感知主机资产风险、安全事件态势，帮助用户全面掌控整网安全趋势。通过系统行为态势分析、文件运行态势分析和网络访问态势分析的三者结合，构建全新的未知威胁感知模型，提高系统对未知威胁的检测能力。

- 深度追溯

深度追踪安全事件发生全过程，在端点侧全面记录安全事件信息，图形化展示威胁事件的多维度信息关联，包括进程调用关系、网络关系、关键注册表、创建文件行为等，剖析每一个安全事件过程。可迅速定位失陷主机并还原事件发生过程，找到事件原点，使每个事件有据可查，与网络情报共享，形成完整事件证据链，锁定威胁源。

- 安全可视化

采用多视角风险呈现模式，构建出透明可视的安全管理平台，从网络、主机、文件、账户、行为、事件等多个角度深度分析，层层展现，暴露每一个风险点，帮助用户做到安全知己。结合事件深度溯源能力，透析安全事件，帮助用户做到安全知彼。

6. 产品适用场景

6.1. 云主机/服务器安全

弥补传统安全手段在这块的空白，扫清资源池安全管理盲区；解决东西向流量访问控制手段缺乏的问题，符合云等保合规要求；安全事件溯源，切实看清安全问题的来龙去脉，责任界定清晰，主动寻求解决和优化办法。

6.2. 专网业务主机安全

主动安全管理，确保专机专用；安全事件溯源与响应，看清风险主机与具体的风险点，快速响应与优化。

6.3. 工控主机安全

主动安全管理，确保专机专用；锁定业务系统和操作系统环境，避免内外部引入的安全风险；安全事件溯源与响应；，切实看清安全问题的来龙去脉，责任界定清晰，主动寻求解决和优化办法。

6.4. 物联网终端安全

物联网终端接入点管控，风险识别与处置，与智慧城市、平安城市等安全态势平台对接等。