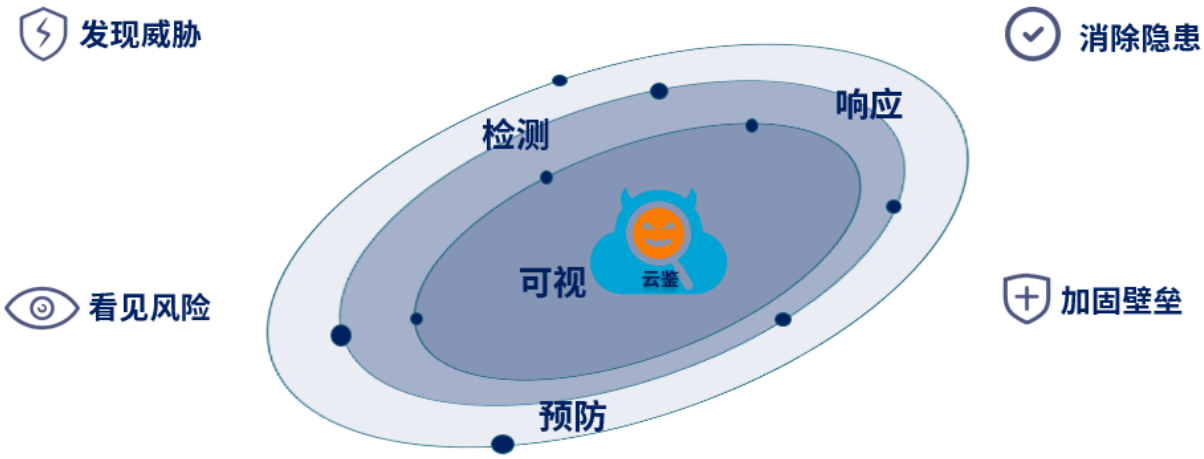
山石网科云鉴主机安全管理系统

随着安全威胁形态的演化，攻击技术不断升级，如：无文件攻击、0Day 漏洞、病毒加壳逃逸，甚至于衍生出勒索及服务的产业链，给企业带来严重损害和威胁。面对网络攻击，传统端点安全产品通过静态特征库匹配来处置威胁，对利用变种恶意软件、新型攻击工具等发起的高级威胁攻击，无法有效防御；随着业务上云和各类终端接入互联网，将有更多的开放端点成为攻击者攻击的目标，这无疑给运维人员带来更大的压力。而智能化、全面化、实时性的主机安全检测机制是应对高级威胁攻击的制胜之道。

山石网科云鉴主机安全管理系统，围绕主机检测、响应、预防可持续安全运营，实现主机安全全生命周期管理。通过对主机进行脆弱性检测、东西向微隔离管控、多锚点风险检测、多层级安全响应等措施，解决主机资产管理、安全加固、东西向流量防护、威胁实时检测、应急响应、失陷主机定位等安全问题，能够有效帮助安全管理人员应对日趋严峻的主机风险态势。



产品亮点

未知威胁检测及防护

不同于传统端点基于静态特征匹配的防护手段，通过机器自学习技术，全网横向对比分析，发现主机异常行为，实时检测与分析入侵点和感染途径，并全网排查感染主机，及时进行威胁处置。

入侵威胁深度溯源

实时对黑客入侵主机过程进行“行为画像”，展示威胁事件来源、传播途径、影响主机数量范围等。

自适应微隔离

提供东西向网络微隔离，构建业务安全边界，解决东西向流量防护难题，实现跨平台安全域的建立。

资源运行智能调度

根据主机系统资源的使用情况自适应调整任务执行队列，当主机处于资源占用高峰状态时，在保障安全防护的情况下对非关键操作可自动延时处理，最大化保障业务处理的计算资源。

多平台兼容性

全面兼容Windows、Linux以及多个国产操作系统，同时支持在VMware ESX、Hyper-V、XEN和KVM等多种虚拟化平台部署，适用于物理环境和虚拟化云环境，建立一体化主机管理与防护平台。

轻资源占用，零打扰

探针占用主机资源极低，运行过程终端用户无感知，并可采用工具批量静默安装，简单快速实施，且系统界面上无弹窗打扰。

产品价值

发现威胁

- 全面资产盘点
- 多维度风险检测
- 实时安全监控

消除隐患

- 快精准威胁溯源
- 多层级安全响应

加固壁垒

- 东西向微隔离
- 可信特征管理

看见风险

- 安全态势总览投屏
- 资产威胁多视角展示

功能规格

主机资产管理

- 支持主机硬件与系统信息统计，资产变更记录，且数据可导出
- 主机自动分组，支持以 IP 地址自动分组，降低管理人员手动运维工作量
- 对主机硬件、网络配置、用户账户等变更进行记录，可记录变更前后内容，并能对关键资产变更进行告警
- 统计 windows 系统安装软件和补丁列表，并能统计全网覆盖情况
- 对每个终端安全状态进行安全评级，可展示具体评级规则
- 自动发现网内未安装探针的主机，可获取主机的 IP 和 MAC 信息，帮助管理员对安全防护遗漏的主机做管理
- 支持 Linux 批量部署，通过管理平台选择未注册主机，进行远程批量部署

主机风险识别

- 基于等保 2.0 以及工信部[YD/T 2701-2014]要求内容，制定涵盖 Windows、Linux 两大平台操作系统的安全基线检查模板
- 支持系统弱密码检测，可自定义弱密码字典，支持批量导入
- 支持网站后门文件检测及隔离
- 对主机实时运行的程序做安全检查和风险评估，帮助管理员快速掌握运行文件安全信息
- 支持 Linux 关键目录下的关键配置文件变更监控，并能获取文件内容
- 支持对注册表安全检测、注册表变更记录、系统日志审计、系统权限篡改检测，对映像劫持、创建自启动项、计划任务程序、驱动程序等进行检查和实时监控，可上报注册表变更记录

主机安全响应

- 基于文件行为和特征的主动防御型查杀，可对已知和未知病毒、木马、勒索、挖矿、钓鱼等恶意程序进行拦截
- 通过识别勒索软件加密动作，实时拦截加密行为，降低文件被加密的概率，减少损失
- 实时监控主机进程资源异常占用并告警，对通过系统程序注入挖矿程序执行挖矿操作的行为提供专项防护
- 对通过系统漏洞、系统进程等执行恶意命令的攻击行为进行识别和拦截
- 依据主机被攻击的情况，通过定制化响应脚本，一键批量响应处理，对顽固病毒进行清除、系统异常修改进行恢复

- 实时监控主机关键的风险入口，对浏览器攻击、office 攻击、系统漏洞攻击、WEBshell 攻击、注册表异常修改等风险行为进行防护
- 对系统关键目录和指定目录及文件进行监控保护，禁止无权限的修改和写入，并能记录违规操作日志
- 通过设定主机运行的白名单，达到除白名单外的文件无法运行，同时内置主机黑白名单提取工具，方便管理员快速提取并生成主机白名单模板
- 支持对网站后门防护，可实时监控和定时扫描，指定需要监控和扫描的具体路径

网络入侵防护

- 实时拦截主机网络侧的攻击，支持端口扫描、泛洪攻击、TCP 洪水攻击等安全防护，并能过滤信任 IP
- 实时检测并告警非法 IP/账号登录行为，支持手动配置服务器合法登录 IP/账号，发现非法 IP/账号登录，及时告警
- 支持身份认证暴力破解检测和防护，可自定义监测方式、自定义处理方式

主机安全运维

- 提供应急响应和远程运维，可远程对主机进行隔离操作、重启操作，以及对探针进行禁用操作
- 基于主机维度，实施双向网络访问控制隔离，同时适用于物理环境和虚拟化云环境，并能对违规访问溯源
- 查看主机正在运行的进程，并能做进程停止操作，以及进程文件隔离和删除
- 远程查看主机的磁盘目录，以及目录下的文件，并能做文件隔离操作
- 支持文件黑白名单和证书黑白名单管理
- 可限制主机不允许使用移动存储设备，帮助管理员规范移动存储设备的使用，减少因违规使用移动存储设备带入风险
- 对系统实时进程中的 CPU、内存使用状态监控，并能筛选高利用率的进程
- 指定路径下指定文件进行全网搜索，方便管理员快速定位在全网潜伏的恶意程序

主机安全审计

- 具备多种畸形报文攻击防护
- 对主机操作的命令进行审计，包括通过 bash、cmd、svchost 等执行的命令，并能对异常命令进行识别告警
- 记录主机实时登录状态和历史登录日志，帮助管理员实时掌握全网主机登录状况，快速发现被异常登录的主机
- 对文件的运行轨迹记录，可追溯恶意文件的传播轨迹，并能记录网内新运行的文件，形成趋势图
- 记录主机网络访问行为，并对网内新增的网络访问进行记录和分析，形成趋势图

安全分析可视化

- 支持图形化展示全网主机安全状况，从终端、事件、资产、网络多个维度展示相关数据，显示风险主机及事件的数量、安全等级和分布情况
- 对全网主机安全状态进行大屏投放，便于运维人员实时监控
- 安全事件详细记录，包括源、目的 IP 端口、关联主机、关联文件、网络访问记录等，并对风险文件调用关系以树形结构展示，可追溯来源与扩散范围
- 对 Linux 主机执行的高危命令进行追溯，可记录事件类型、执行命令内容、执行命令时间、执行命令的用户名，并能查看命令上下文信息
- 基于主机维度将事件、文件、网络、注册表、登录、命令审计日志、资产变更等信息关联汇总，可拖动调整时间轴，对事件发生期间主机内各项变化进行汇总关联分析，还原事件全貌

安全平台运维管理

- 支持数据备份与恢复，可多机冷备管理
- 记录管理员操作日志，可对比每次操作前后配置信息变化情况，对违规操作进行追溯
- 实时监控管理平台资源使用状态，包括 CPU 和内存的实时使用率、管理平台关键服务的运行状态
- 自定义条件查询相关日志，支持以 CSV、JSON 格式导出日志
- 支持 syslog 方式与第三方平台数据共享对接
- 支持邮件告警
- 支持下发各种任务，查看任务执行状态

官方微信　　官方微博