山石智·感 - 智能内网威胁感知系统

—— 有效适用于企业内网的风险态势感知

BDS-i 系列 | BDS-I2850 / BDS-I3850

传统网络安全技术注重边界防御，但针对性、定制化的高级恶意软件已经成为企业的最大威胁，这些高级恶意软件通过逃逸技术处理后，基于签名特征的传统安全技术将无法进行有效检测。据统计，82% 的恶意软件活跃时间仅为 1 个小时，70% 的病毒只出现过一次，这意味着恶意软件在频繁的发生变种。

黑客通过社会工程学攻击，利用变种恶意软件突破了边界防御，或是利用其他手段绕开边界（U 盘带入或私接 WiFi 带入），就可以低成本、短时间、高效率的攻陷内网主机，再通过 C&C、扩散、提权，最终达到窃取敏感数据或破坏核心业务的目的。

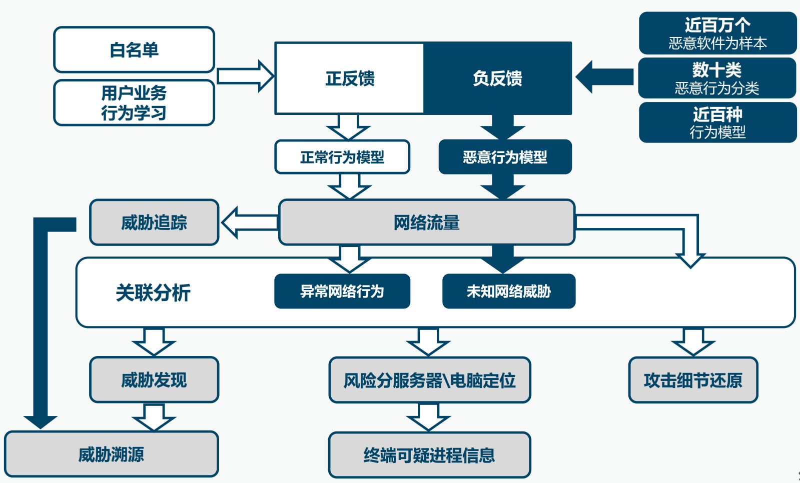
新的网络安全时代，安全体系需要以纵深部署、攻防对抗的思路来构建。内网安全，无疑是攻防对抗的关键举措。通过具备行为分析的智能化安全技术，在第一时间发现内网失陷主机，感知核心资产服务器的风险态势，是部署内网安全最为重要的一步。

山石网科 BDS-I 系列智能内网威胁感知系统，聚焦于内网风险态势感知，致力于核心业务安全。采用山石智能安全技术，重点监控核心资产服务器，检测发现已知及未知网络威胁，精准定位风险服务器和风险主机，同时进行完整的攻击链行为细节还原，构建可视、可管理、可信任的安全内网。

产品亮点

山石的智 · 感集成了基于静态签名技术的 IPS/AV 检测引擎、基于攻击行为分析的高级威胁检测引擎、基于主机和服务器行为建模的异常行为检测引擎，基于蜜罐技术的威胁诱捕检测引擎，以及统一威胁关联分析引擎，全面立体化感知内网风险态势。

- 实时检测内网已知及未知威胁，精准定位异常网络行为的风险主机及服务器；使内网安全可信任，可管理。
- 识别监控内网主机及服务器业务流量，透视核心资产东西向威胁及异常流量，基于内网攻击路径进行分析、溯源、取证；核心资产服务器流量和威胁双向维度深度可视化，充分还原攻击细节。使内网安全可视其形，可明其理。
- 可配置生成内网安全评估报告，全面掌控内网风险态势；支持一键式安全处置，联动边界 NGFW，形成内网安全闭环，简单、快速、高效部署安全策略。使内网安全可控制，可预防。
- 内网安全态势投屏监控，掌握内网安全状态及风险变化趋势，实时发现网络威胁及异常流量访问。



产品核心价值

服务器可视化监视

未知变种威胁发现

失陷主机精准定位

攻击过程细节追踪

终端威胁溯源取证

威胁联动响应处理

功能规格

异常行为检测

- 基于建立主机和服务器行为为数据模型的异常行为检测
- 精准定位内网失陷主机及风险服务器，通过证据报文溯源攻击细节
- 支持配置异常行为检测的灵敏度、学习周期、学习基值等属性
- 支持手动配置学习和不监测，应对业务变更或特例情况

高级威胁检测

- 基于高级威胁行为集的未知威胁检测
- 支持2000多种高级恶意软件家族的检测，包含Virus、Worm、Trojan、Over ow等类型
- Advance Malware Family特征库支持网络实时更新

威胁关联分析

- 基于高级威胁、异常行为和应用行为之间的潜在关联性检测
- 支持不同的数据源查询和执行周期
- 支持多维度关联分析规则库的云端同步

网络层攻击检测

- 多种畸形报文攻击检测
- SYN Flood、DNS Query Flood等多种DoS/DDoS攻击检测
- 支持ARP攻击检测

入侵攻击检测

- 基于签名状态的高性能攻击检测
- 实时攻击源IP 检测、攻击事件记录
- 支持针对HTTP、SMTP、IMAP、POP3、VOIP、NETBIOS等20余种协议和应用的攻击检测
- 支持缓冲区溢出、SQL注入和跨站脚本攻击的检测
- 支持自定义入侵防御特征，提供预定义防御配置模板
- 提供8000多种特征的攻击检测，特征库支持网络实时更新

病毒检测

- 基于流的病毒检测
- 支持压缩病毒文件的扫描
- 超过200万的病毒特征库，病毒库支持网络实时更新

威胁诱捕

- 本地设置蜜罐陷阱，诱捕网络威胁攻击，确认威胁来源、威胁类型及影响范围
- 支持伪装成WEB、文档、数据库等服务器，支持FTP、HTTP、MYSQL、SSH、TELNET五种网络协议

威胁追踪溯源

- 支持对端口扫描、暴力破解、HTTP错误响应等威胁事件进行威胁追踪，记录并展示攻击者的每一次攻击动作
- 支持威胁溯源，联动终端侧部署的sysmon服务，根据五元组信息定位到产生威胁的相关进程

威胁可视化

- 风险服务器、风险主机、威胁事件监控及趋势变化和外部攻击地理分布概览的可视化呈现
- 通过透视镜呈现内网服务器和主机的网络威胁和异常互访流量风险，支持基于TOP10列表添加透视滤镜
- 风险服务器和主机威胁信息可视化呈现，支持识别名称、操作系统、浏览器，服务类型，统计记录威胁行为及异常访问流量
- 服务器和主机基本信息、风险指数、6种IOC（Indicators of Compromises，主机及服务器网络行为技术指示器）威胁行为和互访流量的可视化呈现
- 支持网络威胁检测的可视化呈现，包括威胁名称、威胁类型、风险级别、知识库、证据报文等信息，支持多维度的条件过滤
- 支持投屏监控，包括对全网威胁指数、威胁级别分布、威胁地理分布、服务器异常流量、风险服务器/电脑、威胁事件的集中呈现

威胁处置

- 管理员可针对威胁事件进行忽略、误报、已确认、已修复的仲裁操作，标记威胁事件的管理分析状态
- 支持将威胁事件加入白名单，进行威胁检测特征处理，并通过威胁白名单列表呈现威胁名称、命中数、状态等信息
- 支持针对威胁事件联动山石网科边界安全产品进行防护控制，并通过风险减缓措施列表呈现管理员确认威胁生成的联动防护策略
- 可基于风险主机和风险服务器进行威胁事件的单件或全部删除

应用分析

- 可识别超过3000种以上的PC及移动端应用程序
- 能够准确识别IM、P2P下载、文件传输、邮件、在线游戏、股票软件、流媒体、非法信道等应用
- 支持基于安全域、接口、地域、用户、IP地址等多维度统计

监控告警

- 支持设备CPU、内存、温度、硬盘、物理接口等状态监控
- 支持设备整机流量、新建、并发连接的趋势监控
- 支持设备条件告警，包括CPU利用率、内存利用率、磁盘空间利用率、新建连接、并发连接、接口带宽、机箱温度、CPU温度
- 支持基于应用的带宽和新建连接告警
- 支持Email告警方式

日志报表

- 支持安全威胁、网络流量和设备运行三种预定义类型报表生成任务及自定义报表任务
- 支持即时报表生成及PDF格式文件的导出
- 支持Email和FTP两种报表输出方式
- 支持记录事件日志、网络日志、配置日志和威胁日志
- 支持Syslog和Email的日志外发方式
- 支持基于风险服务器/电脑生成威胁评估报表

集中管理

- 支持本地集中管理审计，将设备注册到安全管理平台HSM，由HSM集中监控多台设备的运行状况及网络流量和安全日志
- 支持云端监控，将设备注册到山石云·景云服务平台，通过手机APP或Web方式实时集中监控多台设备状态、网络流量及网络威胁
- 支持对接第三方威胁情报库，进行恶意文件、恶意URL、恶意IP地址的确认查询检测

关键指标

指 标	BDS-I2850	BDS-I3850
		
应用层处理性能 (1)	2Gbps	5Gbps
存储	1TB	1TB
千兆电口	4个，最大可扩展12个	6个，最大可扩展22个
千兆光口（SFP插槽）	最大可扩展8个	最大可扩展16个
万兆光口（SFP+插槽）	最大可扩展4个	最大可扩展8个
接口扩展槽位	1	2
可选扩展卡	可选配4电、4SFP、8电、8SFP、4电+4SFP、2SFP+、4SFP+	可选配4电、4SFP、8电、8SFP、4电+4SFP、2SFP+、4SFP+
带外管理口	2	2
串口	1（RJ45串口）	1（RJ45串口）
USB接口	2	2
机架高度	1U	2U
电源数量（AC）	1	2
电源（AC）	100-240V	100-240V
频率	50/60Hz	50/60Hz
输入电流	3~5A	3~5A
平均功率	250W	350W
工作温度	0-40° C	0-40° C
储存温度	-40～70° C	-40～70° C
工作湿度	5 ~ 85% 非凝结	5 ~ 85% 非凝结
深宽高(W×D×H, mm)	430 x 375 x 44mm	430 x 500 x 88mm
净重（Kg）	7KG	12KG
毛重（Kg）	10KG	16KG

注：(1) 应用处理性能是在威胁感知功能开启下，混合应用流量的测试结果，实际结果可能会因版本和部署情况而异。

(2) 使用Sysmon需要部署Sysmon服务器及终端插件，用户需自行准备安装环境。Sysmon服务器支持在VMware Workstation、VMware ESXi中部署，终端插件支持在Windows 7/ Windows server 2008及以上版本中安装。