



RG-BDS 大数据安全平台



如有疑问
扫一扫在线咨询

Ruijie 锐捷
Networks

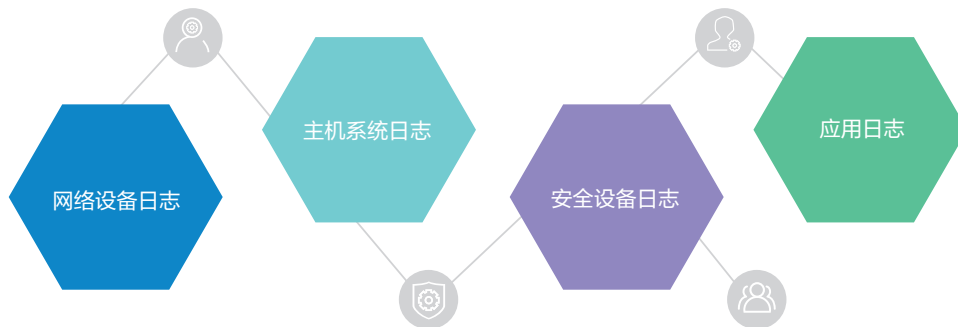
产品概述

锐捷BDS大数据安全平台，应用于教育、政府、医疗、交通、企业、金融等行业数据中心，利用大数据技术解决用户信息安全事件难预警、难定位等问题。BDS兼容市场大多数品牌的安全设备、网络设备、服务器、主机系统、中间件等。可视化呈现网络安全态势，为客户提供简单快速的网络安全分析与运营。

产品特性

收集并标准化海量日志 构建安全大数据仓库

- 服务器、网络、安全等各类日志统一收集。支持SYSLOG、SNMP、FILE、DATABASE、SMB、WMI等多种协议，无需安装代理。
- 安全大数据仓库，海量日志标准化为统一格式。兼容第三方设备（内置支持69家厂商产品型号、300余种日志标准化策略），支持现场编译自定义接入解析，快速落地构建大数据仓库。
- 完美支持IPV6，单套系统支持IPV4和IPV6两套网络。漏洞扫描、基线检查、安全事件接入等全面支持IPV6，实现无缝切换IPV6网。



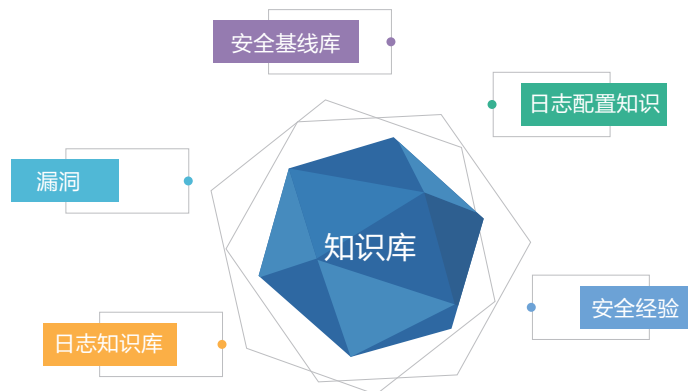
大数据分析 精准定位全网核心风险

- 日志、漏洞和资产大数据关联分析，综合分析风险的整个路径，精准定位安全问题，实现10000:1（日志条目：高危风险）超高收敛比。
- 丰富的关联分析模型，支持自定义，满足各种场景需求。系统提供图形化的关联规则工具，支持基于因果的状态关联分析，用户可根据需求自助完成分析模型。
- 内置漏扫引擎，按需进行漏扫计划。分权分级、定时实时漏扫，自定义漏扫策略，支撑定期安全检查。



构建安全知识库 降低运维技术门槛

- 内置工单系统，流程化安全管理,可以自创建或通过告警、预警转为工单处理, 对问题处理过程进行监控、统计和复查。
- 安全知识库，给技术人员提供技术和解决方案。系统安全知识库，涵盖漏洞、基线问题、安全事件等处理方法。
- 知识库自行管理并不断丰富，提供更新服务。知识库自行扩建和补充，根据用户行业属性积累经验，打造用户专属经验知识库。



安全合规自查 等保自评轻松实现

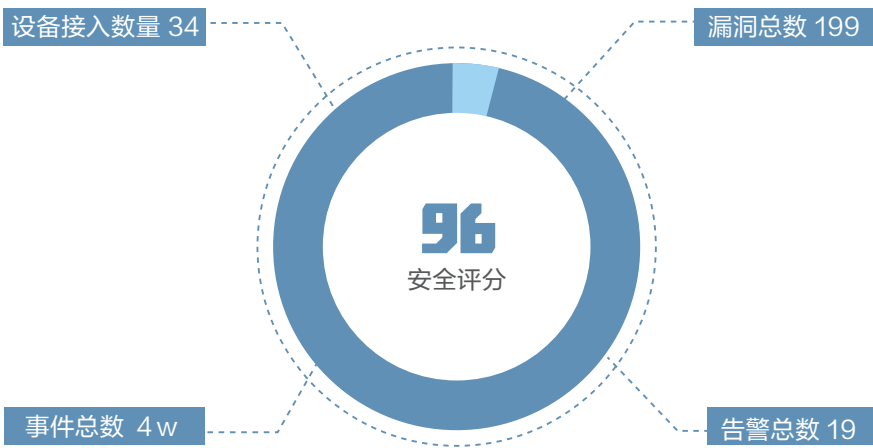
- 基线扫描引擎，实现资产脆弱性感知和自查。基线扫描全面支持主流操作系统、网络、服务器等软硬件设备。
- 脆弱性报表，方便周期性安全检查。支持周期性扫描计划，支持报表自学习经验对比。
- 内置等级保护、萨班斯等标准匹配模型，帮助用户自我测评。基线和漏洞检查结果与内置的国家标准进行智能匹配和测评。



可视化安全业绩 多维度展示建设成果

- 安全日志、漏洞、风险、基线等多维度分析，量化全网安全概况。风险计算模型结合风险等级、资产重要性、系统脆弱性等多个维度的权重要素，为全网安全打分。

- 告警、工单、基线等趋势图，呈现安全建设业绩。配备安全仪表板，集中展示安全要素趋势图，根据需求自助调整布局和内容。
- 现网高危风险展示，实时感知安全态势。展示TOP5高危告警、漏洞。



联动第三方设备 实现整网安全

- **SFlow流日志联动：**通过3000:1采样比，实现东西向问题溯源（兼容三方，只需交换机支持标准SFlow协议）
- **出口NAT日志联动：**通过接入NAT转换前的源IP地址、源端口等关键信息来识别真实攻击源头
- **SMP设备联动：**与认证系统（SMP/SAM）联动实现实名制的日志留存和安全问题定位
- **交换机/路由器联动：**与核心交换机/核心路由器联动实现针对高危敏感命令的操作审计并产生告警
- **RIIL联动：**与运维监控管理系统（RIIL）联动对接，实现安全告警数据和运维监控管理数据（RIIL）统一综合可视化展示，达到安全运维一体化管理、一体化展示
- **SDN联动功能：**与SDN控制器联动实现发现问题、一键智能阻断



技术参数

软件环境	
RG-BDS系列软件版本为一体化安装，软件集成了操作系统，无论虚机还是物理服务器均无需准备操作系统，安装准备环境为Linux，其他引导盘和RAID盘用户按需准备。	
硬件环境	
内存	≥32G内存
硬盘	≥2TB硬盘空间
CPU	Intel Xeon 8核或等同处理能力的CPU

订购信息

型号	描述	备注
RG-BDS-C	大数据安全平台基础版，自带200个监控节点授权，可对日志进行收集、统计与分析（系统自带三年服务授权，到期后无法更新特征库，知识库，策略库，产品可继续使用）。	软件
RG-BDS-A	大数据安全平台增强版，自带200个监控节点授权，最大支持监控节点授权数和服务器的配置有关，可对日志进行收集、统计与分析，同时还可收集系统漏洞，通过大数据关联分析提供全面的安全评估、安全分析与安全威胁等（系统自带三年服务授权，到期后无法更新特征库，知识库，策略库，产品可继续使用）。	软件
RG-BDS 500E-C	日志审计平台硬件版，用于满足等保日志合规要求。自带20个监控节点授权，可扩容至100监控节点授权（每天接收日志量不大于20G），可对日志进行收集、统计与分析，设备自带三年服务授权	硬件
RG-BDS 5000E-A	大数据安全平台增强版软硬一体化设备，2U机箱，配置32G内存，8T硬盘，日志采集性能5000EPS，自带100个监控节点授权，可扩容授权节点至150个，可对日志和流量探针数据进行收集、统计与分析，同时还可收集系统漏洞，通过大数据关联分析提供全面的安全评估、安全分析与安全威胁等。	硬件
RG-BDS-C-LIS-1Y	大数据安全平台基础版服务授权1年，适用于RG-BDS 500E-C、RG-BDS-C产品。	授权
RG-BDS-A-LIS-1Y	大数据安全平台增强版服务授权1年，适用于RG-BDS 5000E-A、RG-BDS-A产品。	授权
RG-BDS-LIS-100	大数据安全平台的100个监控节点授权，支持RG-BDS 5000E-A型号\RG-BDS-A的监控节点授权扩展。	授权
RG-BDS定制开发服务	大数据安全平台定制化开发服务，收费方式为人/天。	服务



锐捷网络股份有限公司

欲了解更多信息，欢迎登录www.ruijie.com.cn，咨询电话：400-620-8818

*本资料产品图片及技术数据仅供参考，如有更新恕不另行通知，具体内容解释权归锐捷网络所有。