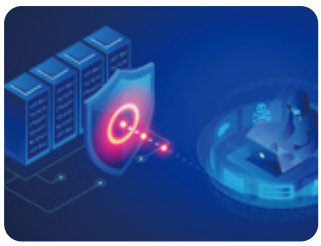
永达电子

主机集中审计平台



产品简介



永达主机集中审计平台是一款安全、高性能的与硬件系统深层结合的主机审计产品，可实现对主机操作系统、软硬件变更、文件使用、外围设备使用等操作事件的管理与审计，改善系统性能，提高安全管理水平。

产品功能

采集策略设置

可对主机审计事件进行采集频率、采集路目录等的策略配置，并可使用分级策略加以区分事件的安全级别。

自身安全功能

支持用户唯一性标识、属性定义、可信管理主机身份鉴别等自身安全保护功能，支持鉴别数据保护、远程管理数据保密。

事件行为监控

对主机的事件与活动行为的监控，并进行审计分析，形成审计日志信息进行上报。

统计分析报表

对审计记录进行统计分析，形成集事件类型、源地址、目的地址、事件描述、风险等级等信息的统计报表，支持查询、导出与自动备份。

主机事件审计

对主机事件、系统活动和用户活动等日志信息进行检查和审计，支持日志重要信息的解析、筛选、导出。

角色权限管理

角色权限默认三种：管理员、审计员、日志员，对系统权限进行有效分权控制，保障日常管理的安全与效率。



永达主机集中审计平台

产品优势

多平台支持

适应多数主流操作平台运行的独立软件包，如Windows、Linux等。

高效数据处理

实现轻松处理海量的日志数据，可支持秒级解锁。

采集终端扩展

单个系统可支持多个采集终端，并可支持集群扩展。

海量数据存储

数据压缩比高，占用存储空间 可实现海量数据的高效存储。

证据保全可溯

实现日志证据保全，支持取证溯源，为事后追责提供有力的保障。

性能参数

部署环境

硬件环境	软件环境
CPU：2核及以上 内存：≧4G 硬盘：≧1024GB	操作系统：CentOS 应用系统：永达主机集中审计平台软件光盘

性能参数

指标名称	指标参数
存储容量	1TB，可支持扩展
每秒钟采集事件入库条数	2000+
控制台并发数	500+
支持采集终端数量	单台支持100+，集群扩展可支持3000+

深圳市永达电子信息股份有限公司
Shenzhen Y&D Electronics Information Co., Ltd.

深圳市永达电子信息股份有限公司，成立于2001年，是一家致力于研发先进计算方法与体系架构的国家高新科技企业。公司以“先进计算+通信”为技术支撑，构建大安全蓝图，服务于“网络空间安全”、“轨道交通安全”、“城市智慧交通”等领域，是中国在智能制造方向的战略科技力量之一。

★ 国家级高新技术企业
★ 国家信息安全服务二级资质企业
★ ITSS二级资质企业
★ 中国保密协会常务理事单位
★ 涉密信息系统集成甲级资质企业
★ 中国网络空间安全协会常务理事单位

地址：深圳市南山区科技北一路17号摩比天线大厦5楼
电话：0755-26727588　传真：0755-26727593
邮箱：sales@s-ec.com　官网：http://www.s-ec.com

售后热线 400-884-0006

*永达电子因产品更新及改进，内容和参数上如有变动，恕不另行通知。本册最终解释权归永达电子所有。