永达电子

安全可信主机风险管控器

产品概述

安全可信主机风险管控器是一款基于「可信计算」理论的内网主机安全管理产品，以安全密码为基因，以身份识别为基础，以资产基线为核心，以监控审计为辅助，以文件为最小管理单元，对主机计算环境实施静态可信和动态行为可性的强制访问控制，构建主动免疫可信架构，守卫纵深防御体系的「最后一公里」安全。

产品功能

01 - 可信运行环境安全度量

- 基于可信安全度量对计算设备系统程序、重要配置文件和应用程序等进行可信验证，通过可信验证，保证运行系统和应用的完整性，从而确定系统或软件运行在设计目标期望的可信状态，确保硬件资源、操作系统、业务软件和配置文件的可信。

02 - 可信标记访问控制

- 支持授权主体（用户级或进程级）配置控制策略，防止非法用户、非法进程的活动。

03 - 可信应用防护

- 具备对业务应用的安全防护功能，可对访问业务程序及数据的行为进行控制，对应用访问资源与数据进行权限控制。保障业务应用相关的数据不被非法篡改和注入，有效保证业务域的配置文件、动态库和业务数据安全。

04 - 可信基线管理

- 自动发现和收集主机上的硬件信息、软件信息、网络配置信息、服务启动信息、进程信息、网络监听端口、系统用户等资产信息，跟踪资产信息变化，提交可信度量基线，对非授权的资产变更产生报警。

05 - 重要文件恢复

- 系统根据策略定时对资产信息进行备份，备份的资产信息包含系统核心运行文件、重要配置文件和管理员自定义的其他目录文件，自动备份时只保存差异文件，并自动构建文件版本号，可查看各版本文件之间的差异以及和基线版本的差异，可手动进行文件恢复，确保文件被发生变更或破坏后，可恢复至正常运行状态。

06 - 异常行为监视

- 通过不间断的采集系统和各类应用运行日志和审计记录信息来进行检测分析，及时发现异常行为。分析并识别已知或未知的威胁，确保在事件发生后提供足够的分析来阻止进一步的攻击。

07 - 运行状态监视

- 实时监视在线主机的运行状态，如：操作系统资源、web 应用、数据库状态等。支持对系统运行状态信息实时查看，当系统运行超出阈值时，可及时发现异常告警。支持对主机进程、服务、用户 / 用户组、文件等的的远程控制。

产品参数

性能指标

1.管理主机节点数50~100个

2.监控指标数≥10000个

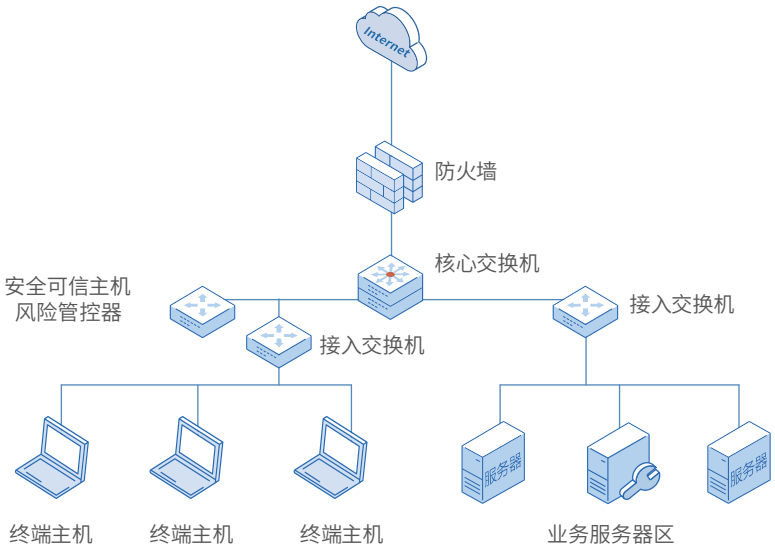
3.每秒处理日志数量100000个

4.控制命令响应时间≤2秒

硬件参数	
形态	3U机架安全设备
管理接口	1 个 10/100/1000BASE-T 管理网口
业务接口	20 个 GE 以太网接口，2 个万兆光口（SFP+）
供电	支持220~240V AC
电源模块	2个热插拔550W交流电源模块，支持1+1冗余
温度	5°C~45°C
尺寸	750*440*133mm

* 规划中产品规格，具体当前可配置信息以详细产品手册为准。

设备部署



产品亮点

统一的安全策略管理

为所管业务域建立统一的管理中心，系统管理责权分离，管理角色分为安全管理员、系统管理员和审计管理员。

分布式集中管理

通过集中管理的方式，既方便管理员管理，同时使管理员能从总体的高度制定内网安全策略，并能及时了解内网安全状况。

科学的安全策略管理

在安全策略管理上，系统还可将策略组和用户组绑定，使得安全管理员可以灵活地将不同安全策略应用到不同用户组中；同时系统支持日志管理员和用户管理员等角色的建立。

持续监控与分析能力

采用自适应安全架构设计，从预测、防御、检测、响应四个维度构建安全能力，符合自适应安全架构的持续监控与分析核心要求，助力客户构建持续响应安全体系。

全面的深度终端监控

系统提供硬件、软件、操作系统账户、注册表项的安装/卸载变化监控；提供终端在线状态、在线时长、违规内外联的监控；提供终端设备使用情况、共享情况、拨号情况等监控等。

安全可信管控服务

在线状态监测、系统资源监测、软件情况监测、进程监控与审计、服务监控与审计、网络端口监测、打印监测、上网情况监测、违规外联监测、文件检测、主机安全策略监测、主机桌面监测等。

多维安全能力协同联动

结合虚拟沙盒等技术，通过安全体检、安全监控、漏洞风险、入侵威助等多个功能模块的联动，以及模块间数据的联通，形成闭环系统，为企业提供全方位、强有力的安全防护。

采用轻量级Agent

具备主机安全所需全部功能的最小集合，Agent占用资源极少，功能丰富、性能稳定，不影响主机系统的正常运行；支持动态升级和更新；可根据业务的负载进行弹性调整。

客户案例

国家部委

- 中共中央统一战线工作部
- 中华人民共和国工业和信息化部
- 中华人民共和国应急管理部
- 中华人民共和国科学技术部

地方政府

- 北京市东城区人民政府
- 成都市应急管理局
- 深圳市发展和改革委员会

国有企业单位

- 中国国家铁路集团有限公司
- 中国十八个铁路局集团有限公司
- 通号通信信息集团有限公司
- 北京经纬信息技术有限公司

本产品符合国家标准：

- GB 42250-2022《信息安全技术 网络安全专用产品安全技术要求》
- GB/T 38638-2020《信息安全技术 可信计算 可信计算体系结构》
- GB/T 20278-2022《信息安全技术 网络脆弱性扫描产品安全技术要求和测试评价方法》（增强级）
- GA/T 910-2020《信息安全技术 内网主机监测产品安全技术要求》（增强级）
- GA/T 403.2-2014《信息安全技术 入侵检测产品安全技术要求第 2 部分：主机型产品》（增强级）

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

★ 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　★ 涉密信息系统集成甲级资质企业

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