

★完全公

开

奇安信网神零信任 身份分析系统(IDA)V2.0- 产品彩页

地址：北京市西城区西直门外南路26号院1号
邮编：100044

1 产品概述

奇安信网神零信任身份分析系统 (IDA: Identity Analysis) 是在企业应用及 API 服务访问场景中,为了解决用户的访问设备环境变化及动态行为可能引入的安全问题而推出的一款安全产品。该平台主要针对访问控制的实时性要求,采用了大数据分析、机器学习、偏离度算法、可视化展示等多项核心技术,对用户持续访问过程中的环境安全及行为安全进行分析并进行风险响应,为企业提供了访问设备环境分析、用户行为画像、风险分析、持续监控、风险处置能力。同时,奇安信网神零信任身份分析系统(IDA)也是以零信任架构为基础的奇安信身份安全解决方案中的重要组成部分,可基于奇安信网神零信任应用代理系统 (TAP)、奇安信网神零信任 API 代理系统 (TIP)、奇安信网神零信任身份服务系统 (TAC) 的日志进行用户行为以及基于奇安信网神零信任环境感知系统 (TESS) 的设备环境信息进行风险分析和信任评估,为动态访问控制提供执行依据。

奇安信零信任身份分析系统支持国产化,CPU 满足 24 核,256GB 内存,32TB 存储空间,采用国产化中间件、数据库和操作系统。

2 产品功能

2.1 风险汇聚功能

奇安信网神零信任身份分析系统(IDA)可提供日志大数据汇聚、存储及管理能力,为日志服务提供数据支撑。

- 提供风险汇聚的功能,接收来自认证服务、权限管理服务、审计服务、安全防护策略控制服务上报的风险信息;

- 内置了安全事件的详细分类信息，只有被系统识别，并且能归类到系统事件分类中的事件，才会被响应；
- 在事件的识别方面，提供精确匹配、模糊匹配、正则表达式、自然语义处理等多种技术手段，将其他系统发生的事件做分类汇聚；
- 满足《GA/DSJ351-2020 公安大数据安全零信任体系技术设计要求》中业务安全策略控制服务要求。

奇安信网神零信任身份分析系统(IDA)可提供界面化及接口方式的日志数据查询能力，支持精确、模糊、分类、组合、批量等多种查询方式，支持多条件查询和全文检索功能，并且返回数据汇总及明细信息。

2.2 风险关联分析

奇安信网神零信任身份分析系统(IDA)结合用户发生操作的时间、位置、设备、频度、结果以及感知到的设备感知信息等属性定义了多种使用场景下的安全判定规则，从而发现出用户访问活动中存在的潜在威胁。

提供了风险汇聚的功能，可将环境感知服务、业务审计服务、权限管理服务、认证服务和外部安全平台及体系传递的风险信息进行收集、汇聚和关联分析；外部安全平台及体系可以是安全访问与数据交换及安全防护体系等；满足《GA/DSJ351-2020 公安大数据安全零信任体系技术设计要求》中业务安全策略控制服务要求。

2.3 信任评估

奇安信网神零信任身份分析系统(IDA)可有效感知访问终端的环境风险、发现存在安全威胁的账号、设备行为,综合多种安全因素对访问主体的安全性进行信任评估,并且计算出量化的信任级别,以其作为系统安全控制策略的判断条件,或其他外部的访问控制系统提供安全判断依据。

基于风险事件、认证强度、环境提供信任等级评估框架。风险事件不仅考虑奇安信网神零信任身份分析系统(IDA)根据接收的日志进行的风险事件同时将对接的众多第三方平台的风险事件考虑在内。认证强度是对主体身份可信度确认的一个衡量标准,不同信任等级可要求不同的认证方式。环境要求是进一步对主体身份可信度的衡量,主要对设备的要求如受控设备,用户活动信息的匹配要求如常用地理位置。

信任评估模块还提供内置的模版,该模版基于Gartner 的可信身份联合模型及近三年的分级访问控制实践经验得出,4级信任等级划分的要求,同时给出各级信任等级的使用建议,信任等级为低不允许认证通过、信任等级为中允许访问门户等、信任等级为低允许访问低敏应用、信任等级为高允许访问高敏应用。

基于内置模版或自定义的信任等级评估框架,奇安信网神零信任身份分析系统(IDA)实时评估主体信任等级,并可在事后提供信任溯源到具体认证、访问活动日志。

提供了信任评估的功能,可将汇聚的各服务及外部的多维风险信息进行关联分析,形成确定的风险信息,并基于信任评估模型进行综合评估,形成信任评估结果和生成控制指令;基于用户、上下文相关数据进行推断评判,评估过程需要根据用户、终端设备、业务应用、接口等历史数据,形成历史信任数据,根据历史评估可依据历史数据、实时数据进行综合推

断；满足《GA/DSJ351-2020公安大数据安全零信任体系技术设计要求》中业务安全策略控制服务要求。

2.4 控制指令下发

基于神经网络模型、训练算法及动态检测，奇安信网神零信任身份分析系统(IDA)可持续分析 API 调用过程中的行为流量，发现 API 服务中所常见的安全威胁，提供控制指令下发：

提供风险联动通报可支持通过查询接口查询风险信息，并支持通报状态校验机制，避免信息伪造，支持风险信息通报失败重传，避免信息丢失。

提供与外部服务联动的功能，联动主要分为输入和输出联动。输入联动主要来自于环境感知服务环境信息的状态和通知，来着认证服务、权限管理服务、业务审计服务和外部系统的各类风险信息输入；输出联动主要指与认证服务和外部系统的策略控制指令的输出；

满足《GA/DSJ351-2020 公安大数据安全零信任体系技术设计要求》中业务安全策略控制服务要求。

2.5 外部联动认证

奇安信网神零信任身份分析系统(IDA)具备针对风险事件进行动态安全决策的能力。IDA 在以其对风险威胁的分析能力和风险事件的发现能力为基础，进一步为安全访问控制提供了风险处置决策能力。风险策略主要包括风险、执行意图、执行指令（执行者、执行对象、执行命令等）、策略状态，策略状态包括运行和测试模式，运行模式策略直接执行，测试模式再不影响现有访问的基础上，提供策略运行模拟。目前风险策略的触发事件可覆盖设备环

境、用户认证、应用授权及访问行为等类型事件，执行意图包括重置会话、补充认证因子、阻断连接（ip 或用户）、冻结账号、取消权限、冻结设备，通告对象为奇安信网神零信任身份服务系统（TAC）。

- 与认证服务联动

提供接收来自认证服务的风险信息，提供向认证服务发送控制指令，提供认证服务的硬件特征、硬件环境类型和终端风险信息查询；满足《GA/DSJ351-2020 公安大数据安全零信任体系技术设计要求》中业务安全策略控制服务要求。

- 与环境感知服务联动

提供从环境感知服务进行环境信息同步支持接收来自环境感知服务的终端风险信息，能接收来自环境感知服务的信息变更通知；满足《GA/DSJ351-2020 公安大数据安全零信任体系技术设计要求》中业务安全策略控制服务要求。

- 与权限管理服务联动

提供接收来自权限服务的风险信息 and 传递，提供向权限服务发送控制指令，提供接收来自权限服务的权限变更通知；满足《GA/DSJ351-2020 公安大数据安全零信任体系技术设计要求》中业务安全策略控制服务要求。

- 与审计服务联动

提供将系统日志信息上传或同步到审计服务，提供接收来自审计服务的风险信息 and 传递；满足《GA/DSJ351-2020 公安大数据安全零信任体系技术设计要求》中业务安全策略控制服务要求。

- 与安全防护策略控制联动

提供接收来自安全防护策略控制的风险信息，可向安全防护策略控制传递风险信息；满

足《GA/DSJ351-2020 公安大数据安全零信任体系技术设计要求》中业务安全策略控制服务要求。

- 与检查控制点联动

提供查询检控策略信息，提供接收来自检查控制点的各类访问风险信息，提供向检查控制点下发控制指令；满足《GA/DSJ351-2020 公安大数据安全零信任体系技术设计要求》中业务安全策略控制服务要求。

- 与业务应用/应用服务/数据服务进行联动

提供响应业务应用/应用服务/数据服务查询策略信息，提供接收来自业务应用/应用服务/数据服务上报的各类访问风险信息，提供向业务应用/应用服务/数据服务下发控制指令；满足《GA/DSJ351-2020 公安大数据安全零信任体系技术设计要求》中业务安全策略控制服务要求。

2.6 实体画像

实体画像包括用户和设备画像

1. 用户画像包括群组画像和个人用户画像

1) 群组画像基于用户组或全体用户的用户日志、访问日志刻画行为基线，包括使用设备数分布、操作系统类型分布、登录城市数分布、访问资源列表、在线时间、会话流量分布、登录地理位置分布等。

2) 个人用户画像包括

- 用户基本信息，包括用户姓名、用户 id、用户组织机构、最近的信任等级、最近活跃时间等

- 风险事件记录，用户关联的风险事件趋势、风险事件分布、风险事件列表
- 统计画像，即用户的行为基线包括用户设备与 IP 关系图、资源分布、请求流量趋势、地理位置分布、在线时间分布等
- 信任等级趋势
- 活动记录，包括用户相关的认证日、访问日志

2. 设备画像包括如下信息

- 设备基本信息，包括设备 id、设备类型、设备归属、设备绑定用户等。
- 设备统计记录，包括设备 ip 与用户关系图、设备风险趋势、设备风险原因分布等
- 设备相关的风险事件记录
- 设备相关的活动记录包括认证日志、访问日志等

2.7 可视化报表

奇安信网神零信任身份分析系统(IDA)可提供多维度的风险分析大屏展示及可视化报表，可对日志大数据分析结果进行量化展示，支持从帐号维度、用户维度、时间维度进行分类展示，以帮助管理人员直观地了解整个监控周期内发生的访问行为是否存在安全威胁。

目前系统可视化大屏展示内容包括：访问流量状态、用户可信状态、设备的可信状态、应用的风险统计、API服务的风险统计，以及风险发生的实时统计。

目前系统可支持基于用户日志、访问日志、风险日志的可视化报表展示及导出，报表内容包括：认证统计、准入统计、访问授权统计、资源访问统计、风险统计、会话统计等并支持按照时间段、源IP、用户、访问目标、访问结果查询展示详细内容，便于实现业务数据的审计、安全风险的溯源。

2.8 外部平台对接

奇安信网神零信任身份分析系统(IDA)对外提供了与其他外部用户行为收集系统对接的能力。通过联动配置以及使用预先定义的接口数据格式，奇安信网神零信任身份分析系统(IDA)可接收奇安信网神零信任应用代理系统(TAP)、奇安信网神零信任 API 代理系统(TIP)、奇安信网神零信任身份服务系统(TAC)上报的日志进行用户行为的风险评估，也可接收奇安信网神零信任环境感知系统(TESS)的终端环境感知数据进行设备风险分析，或者接收其他外部系统提供的风险数据如用户日志或审计记录等，并进行多维度数据汇聚关联，以对安全基线进行优化及执行更加全面的综合风险计算，获取更加准确的风险评估结果。同时，奇安信网神零信任身份分析系统(IDA)也通过接口服务将风险计算结果或风险处置策略提供给其他外部应用或平台。

2.9 集群化部署

奇安信网神零信任身份分析系统(IDA)支持集群化部署，具备高可用性及可扩展性：

- 支持集群设备的负载均衡，提升并发数据处理能力，有效发挥系统的整体效率
- 支持多台设备组成集群，以实现热备份，确保服务的高可用性

- 支持集群化设备数量的水平扩展，可迅速增加奇安信网神零信任身份分析系统(IDA)的计算能力，快速实现扩容，避免重复部署。

3 产品价值

3.1 多维度风险分析，提升威胁感知能力

奇安信网神零信任身份分析系统(IDA)利用设备环境信息及用户日志数据，从设备、时间、位置、结果等多个维度进行环境分析、行为分析，还可与其他外部服务提供的用户信息进行多维度数据关联，以执行更加全面的综合研判，覆盖更加全面的风险场景。通过奇安信网神零信任身份分析系统(IDA)，不仅可以发现设备环境变化可能引入的安全风险，同时也能对帐号所有者无意的风险操作以及帐号被窃取之后发生的内部横向攻击进行感知。奇安信网神零信任身份分析系统(IDA)，可及时感知访问过程中发生的安全威胁。

3.2 风险处置信任评估，提升系统安全能力

奇安信网神零信任身份分析系统(IDA)通过信任评估，做到事前预判场景风险并根据业务安全要求制定分级访问控制策略；通过安全策略，事中、事后都对风险进行有效控制，并且具备及时发现，实时分析，立即处置的特点，全方位的提升系统安全能力。

3.3 提升 IT 安全运维效率

奇安信网神零信任身份分析系统(IDA)可自动化、高效率地对海量用户行为数据进行分析处理，并通过图表向安全运维人员通知风险事件，由此能大幅减少安全运维人员需要处理

的数据量，有效提升企业 IT 部门安全运维效率。