“物联网安全边缘准入网关的研发”成果登记公示信息

成果名称：	物联网安全边缘准入网关的研发
完成单位：	深圳市万网博通科技有限公司
完成人员：	刘健,罗育专,谭志龙,丁鑫,方靓,高勇,李铁牛,喻良,周喜彬,黄涛,李健,郑智进,房李威,旷智威
研究起止日期：	2023-05-08 至 2024-03-22
主要应用行业：	制造业
高新技术领域：	电子信息
评价单位：	深圳市科技中介同业公会
评价日期：	2024-12-30
成果简介：	一、产品简介 本项目产品物联网安全边缘准入网关，集成了终端自动识别、终端授权准入、终端安全风险感知、内网行为分析识别及AI智能运维等技术，这些先进技术为物联网共同构建了一个安全可控、资产明晰、故障可追溯的管理体系，确保系统运行的安全性、稳定性与可靠性。本项目产品拥有数据采集与预处理、协议兼容、边缘计算能力、安全防护等先进性，通过数据采集与预处理功能，网关能够高效地收集并处理来自物联网终端的数据，为后续的分析和决策提供有力支持。同时，其强大的协议兼容能力使得网关能够与多种物联网设备和系统进行无缝对接，实现数据的互联互通；边缘计算能力则使得网关能够在本地对数据进行初步处理和分析，减轻中心服务器的负担，提高系统的响应速度和效率；安全防护功能作为网关的核心竞争力之一，通过多层次的安全防护措施，确保物联网系统的数据安全和运行安全。

	二、技术特点 1.资产扫描 资产扫描：依托智能扫描引擎，采用多种协议解析技术：深度包检测（DPI）、流量特征分析、端口扫描技术有机融合，对目标网络空间进行多层次的探测。并借助 AI 智能识别技术，持续获取设备信息，实现端点设备身份指纹特征的提取和合规性检查，实现对资产全生命周期的动态化管理。 2.接入控制 身份认证：基于零信任网络，建立授权准入信用体系，解决设备身份合法性问题，对前端设备进行身份指纹授权认证，只允许可信资产接入网络，阻断非法资产接入。 3.访问控制 ①边缘计算与智能分析：在物联网接入端部署边缘计算节点，对前端数据进行实时采集和智能分析，减少对中心服务器的依赖，提升对数据的识别能力和识别效率； ②行为基线建立与控制：通过数据采集和统计设备流量，自动识别网络中的正常业务行为和异常行为，建立行为基线，对异常行为的设备，系统会告警并采取控制措施； ③数据清洗与过滤：内置数据清洗机制，将识别出的异常行为根据预设的规则或算法对数据进行清洗，同时还会对数据进行过滤，根据实际需求选择性地提炼有用数据，减少非正常业务数据，提高数据转发效率； ④纵向数据安全防护：针对南北向数据流，通过智能算法，建立起纵向数据流的单向大模型，实现纵向流量的智能过滤，有

	效阻断南北向的网络攻击行为； ⑤横向数据安全管控：针对东西向数据流，通过智能算法，建立横向数据流的双向大模型，实现横向流量的智能管控，有效阻断病毒、木马等网络攻击的横向蔓延。 4.风险探测 风险扫描：支持安全风险扫描引擎，能够检测网络上的主机状态、开放端口、弱口令及安全漏洞。采用多线程技术、定制化扫描策略，提高扫描效率和准确性。 5.智能运维 ①智能运维：依托大数据、人工智能、机器学习等前沿技术，构建起一套高度自动化与智能化的运维体系，广泛、精准地收集各类运维数据，快速识别出潜在的故障，并通过异常检测算法，实时比对当前数据与历史正常数据的偏差，精准定位系统中的异常点，提前预警可能出现的故障隐患。 ②可视化运维：将复杂、晦涩的运维信息转化为直观、易懂的视觉呈现形式，为运维人员提供全方位、实时且精准的运维洞察，进而大幅提升运维效率与决策质量。 6.集中管控 支持物联网安全态势感知平台集中管理统一配置，物联网安全边缘准入网关将自身探测到的安全风险、资产数据及运维的数据统一上报给物联网安全态势感知平台并集中呈现、告警信息统一推送；同时接受执行物联网安全态势感知平台下发的策略。 三、主要技术指标 1.支持 100-5000 个 IP；

	2.资产扫描技术采用分布式，支持大规模并发扫描，能够在短时间内快速覆盖整个网络环境； 3.真正无代理技术，主动探测 5 分钟设备上线完成，10 分钟完成网点资产探测识别； 4.资产探测过程，不会对网络带来明显的影响，通过对所接入交换机 1 分钟 CPU 使用率变化来判定是否对网络带来明显影响，当系统发起探测扫描时，交换机 CPU 利用率不会超过资产探测发起前 5 分钟平均值上下 2%浮动； 5.弱口令字典大于 3000+； 6.指纹库大于 40000+； 7.漏洞库数量大于 300000+； 8.私接终端设备接入网络，10 秒内系统可发出私接告警提示； 9.仿冒设备接入网络，60 秒内系统可发出仿冒设备告警提示； 10.发现私接设备后 10 秒内阻断其访问网络； 11.发现仿冒设备后 30 秒内阻断其访问网络； 12.终端设备离线后，30 秒内系统可发出设备离线告警提示，并定位出设备网络位置。