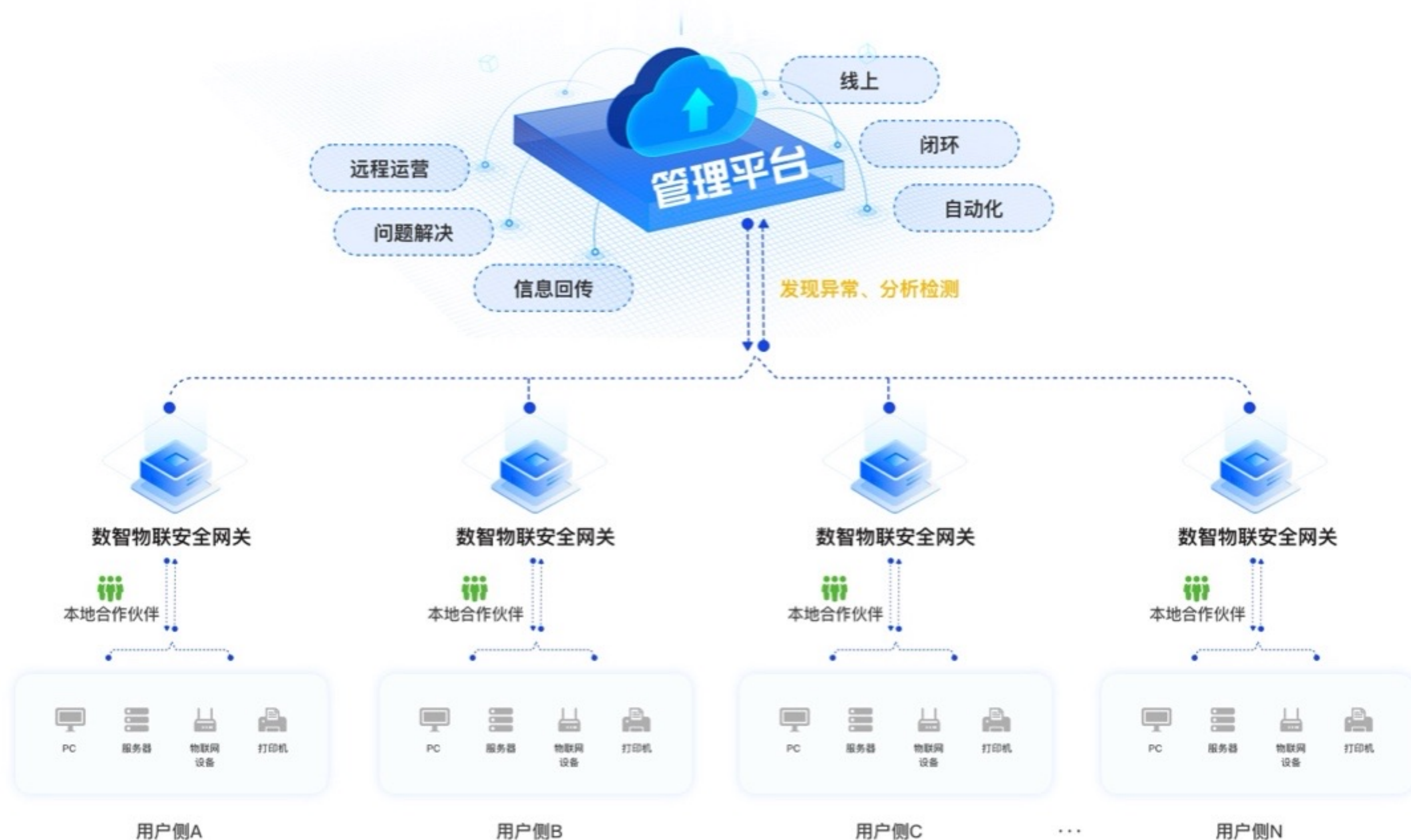


数智物联安全网关



系统介绍

数智物联安全网关，创新性“最小网格化安全管理”理念，构建最小网格化主动防御体系，提供资产探测识别、资产接入认证、资产漏洞管理、主动防御、威胁定位、网络行为管理及跨境VPN代理检测，可帮助政企用户快速建立面向安全威胁的主动化、实战化、常态化的安全防护能力，结合7*24小时云端监测运营，为政企客户提供“识别-控制-评估-监控与响应”的高性价比、一站式资产安全管理方案。



场景痛点

资产管理日益复杂

随着物联网终端数量激增、类型多样化且分布广泛，传统的资产管理方式难以应对其动态接入、状态监控和精准盘点的挑战，使得IT资产管理越发复杂；同时存在上网行为失管所导致的效率低下，私自跨境翻墙可能引发的数据泄露与合规风险。

无法确定最有效的安全投资

在资金预算有限的情况下，安全投入往往面临“广撒网”却难以精准聚焦核心风险的困境，导致资源分散、效果稀释，最终形成“投入持续但防护提升不明显”的被动局面。

缺乏安全管理人员

安全人员短缺，无法建立全天候安全监测和应急保障体系，无法进行及时的响应处置。

一站式解决物联网安全问题

集约化架构替代传统碎片化方案，有效识别针对传统PC、哑终端、智能设备等多种终端，覆盖资产管控、风险检测、边界防护的纵深防护体系，有效应对混合网络环境中的复杂安全挑战。

节省投资 效果可视

多功能一体化设计，大幅减少硬件采购数量和建设复杂度，直接降低初期投入和后续维护成本。向导式安全配置，统一管理界面以及可视化分析工具，使运维操作集中简便，直观呈现安全成效。

云端运营 专属服务

安全网关的本地安全能力与私有云管理平台运营服务结合，构建三级安全运营体系，提供一对一运营专家服务，助力用户打造全天候安全监测和应急保障体系。

解决之道



核心能力



基于AI的行为学习与资产管控

通过主动探测、被动流量分析等方式，自动化全面识别通用办公机、物联网设备等企业多类型IT资产，并进行有效准入控制，解决海量IP设备的接入认证和安全管控问题，帮助用户构建全网终端资产和网络态势的可视、可管、可控。

主动探测技术

探测

类型 ☒ 主动探测 ☐ 被动探测

更新间隔 从不 分钟

* IP 192.168.1.2/19 清空 添加

192.168.1.23/25 清空

排除IP 多个之间用,分隔开

主动扫描状态 停止

被动扫描状态 正在扫描

应用

业务行为建模

序号	源IP地址	目的IP地址	源端口	目的端口	流量长度	数据包内容十六进制显示	数据包内容ASCII显示	注册时间	协议
1	192.168.18.144	224.0.0.251	5363	5363	42	000000000100000000000012	Broadcast control level...	2024-07-02 07:12:34	UDP
2	192.168.18.144	224.0.0.252	5365	5365	36	000000000100000000000012	16... Broadcast control...	2024-07-02 07:12:34	UDP
3	19.16.18.8	19.16.18.5	3472	88	1	003305322011ba9ba796a0717	USER anonymous	2024-06-28 02:16:45	TCP

应用

全终端资产自动识别发现

探测

类型 ☐ 主动探测 ☒ 被动探测

* IP 192.168.1.2/19 清空 添加

192.168.1.23/25 清空

排除IP 多个之间用,分隔开

主动扫描状态 停止

被动扫描状态 正在扫描

应用

被动流量学习技术

全终端资产运行入网、监控、管控

阻断

部署方式 ☐ 串联部署 ☒ 旁路部署

阻断接口 eth1

指纹异常阻断 ☐ 是 ☒ 否

未鉴权阻断 ☐ 是 ☒ 否

应用

提示: 当MAC地址、端口和OS发生改变时, 会触发指纹异常

旁路阻断技术



持续的漏洞监测 随时掌握企业资产漏洞情况

针对企业IT资产进行漏洞检测和漏洞生命周期管理，形成全面多维的风险扫描报告，形成不同时段的风险情况，涵盖受影响的资产、漏洞详细信息，解决方案等。

资产风险全生命周期管理



提供资产的台账梳理、变更记录、运行状态监控、漏洞和风险排查一站式全生命周期管理服务。

资产风险预警



基于资产信息与内置知识库初步判断设备漏洞情况，对系统进行漏洞扫描，支持检查结果与资产信息整合。

直观风险呈现



通过扫描报告输出，提供友好度很高的报告展示系统，支针对目标系统的安全评级、资产信息统计、漏洞分类与统计进行直观展示。



构建主动动态防御 提升攻击成本 降低风险

利用虚拟伪装和动态诱捕技术，构建动态变化的网络环境，虚拟出海量伪装节点和服务迷惑和诱捕攻击者。通过构造虚拟网络增加网络拓扑的随机性和迷惑性，使攻击者找不到攻击目标。



多重安全能力于一体 全面深度防御

- ✓ 防护墙访问控制
- ✓ 入侵监测及防御
- ✓ 恶意样本检测
- ✓ 网络行为管理

安全防护能力

- ✓ 抗拒服务攻击
- ✓ 跨境VPN代理检测
- ✓ IP黑名单
- ✓ Web应用防护

配置入侵防御透明模式_脚本高级防护对象				
输入sid				
基础防护				
用户认证攻击				
木马后门				
拒绝服务攻击				
文件识别攻击				
口令攻击				
缓冲区溢出攻击				
远程访问攻击				
漏洞扫描攻击				
间谍攻击				
网站攻击				
缓冲区溢出				
爬虫攻击				
跨站脚本攻击				
sql注入攻击				
蠕虫病毒				
目录扫描攻击				
WEB扫描				
高级防护				
基础防护 / 用户认证攻击				
#	特征名称	处理动作	是否输出日志	sid
	用户认证攻击	☒ 通过	☒ 全选	
1	[IPSEC] IPSEC protocol detect	☒	☒	21037
2	试图利用7960中已知漏洞时，会产生此事件。	☒	☒	13664
3	当试图利用一个已知的acrobat漏洞时，会产生该事件。	☒	☒	26077
4	企图利用一个在NetBackup数据和商务中心已知的漏洞。	☒	☒	17706
5	试图利用一个已知的漏洞在J2SE。	☒	☒	20820
6	这个事件发生在试图发送一个畸形的通信到互联网协议...	☒	☒	11972
7	尝试利用Adobe Acrobat Reader和Flash一个已知的漏...	☒	☒	15727
8	这个事件时生成试图利用一种已知的漏洞VideoLAN VL...	☒	☒	9844
9	试图利用Acrobat Reader中一个已知的漏洞时，会生成...	☒	☒	23516

1

一站式解决互联网安全问题

全面应对
互联网的主流安全攻击和威胁

2

极简配置 让客户省心放心

极简配置
自激活、自运营、零等待

3

节省投资 帮客户省钱

无需部署多个安全设备
极大节约投入

4

安全可视化专属定制

安全报告和安全大屏
专属定制、极致的服务体验



安全告警自动获取

- ▶ 采用workflow工作流编排
- ▶ 自动获取安全告警数据
- ▶ 安全告警自动截图存证

多重关联分析

- ▶ 攻击IP、被攻击IP自动化解析
- ▶ 威胁情报关联解析



AI大模型自动化分析

- ▶ 利用AI大模型强大的安全分析能力
- ▶ 详细深入进行威胁分析
- ▶ 7x24全自动威胁处理

威胁分析报告自动化生成

- ▶ 智能体生成详细的分析报告
- ▶ 深入解析攻击过程



精准识别跨境翻墙VPN 消除数据泄露与合规风险



自研指纹模型准确识别

利用机器学习和AI行为分析，对各类混淆加密的翻墙VPN协议进行分析与检测，可精准识别Clash、V2ray等翻墙VPN代理工具的网络流量。

跨境VPN 代理检测



情报库快速命中

跟踪Telegram、暗网、github等翻墙VPN供应网络，获取翻墙VPN代理情报数据，建立多维度的翻墙VPN代理情报数据库，快速命中VPN翻墙等违法行为。



关于我们

北京椰子树信息技术有限公司于2015年3月成立，服务政府、能源、运营商等行业大型客户，覆盖中小企业客户。公司致力于构建安心世界，成为主动安全攻坚者，极简安全实践者。

北京椰子树信息技术有限公司是北京市“专精特新”中小企业、国家高新技术企业、中关村高新技术企业。公司专注于采用创新的“积木式”安全架构，基于流量打造业务内生安全，实现自主可控的“从端到云”的全景安全解决方案和服务，推动各类安全组件在信创、合规、护网、新安全应用落地，主攻自主可控安全虚拟化、白盒化产品及服务。