绿盟物联网安全风控平台

产品白皮书

【绿盟科技】

■ **文档编号**	NSF-TR-RPM-081	■ **密级**	完全公开
■ **版本编号**	V2.0	■ **日期**	2019-03-25
■ **撰 写 人**	杨茜	■ **批准人**	

■ **版本变更记录**

时间	版本	说明	修改人

目录

插图索引

一. 物联卡违规滥用形势严峻

物联网在全球呈现快速发展趋势，我国在“十三五”规划中明确提出了物联网国家战略，为信息通信产业开拓了新空间。中国移动基于“十三五”规划提出“全面实施大连接战略”，将万物互联作为战略布局方向，加快物联网建设，预计到 2020 年物联网连接规模超过 5 亿，开放平台连接规模达到 5 亿。中国联通为了实现真正的“大连接”，表示已经把物联网、车联网划入中国联通的 5G 战略里面。中国电信提出转型 3.0 战略，把发展物联网作为重要的发展战略之一。

随着移动技术的不断发展，物联卡成为企业实现物联网管理既简单又有效的方式，物联卡受到越来越多企业的欢迎，物联卡的需求也呈迅速增长趋势。中国移动官方数据显示，2018 年 7 月 30 日 9 点 15 分，物联卡用户数突破 3 亿。中国电信与中国联通，也分别发放了近一亿的物联卡。

在物联卡大规模普及的同时，物联卡存在的问题也愈发凸显。不同物联网业务对短信、话音、数据等基础功能需求存在差异，物联卡在资费方面存在流量池计费、无漫游、资费较优惠等特点，这些卡在销售给客户后存在挪用异常、滥用异常和其他异常等安全风险，可能导致公司经济损失，甚至有被用于通讯信息诈骗，甚至使得公司面临工信部考核问责的风险。目前物联卡违规情况主要包括：

- ✧ 违规挪用：某客户购买卡后，将本应用于 A 物联网业务的卡挪到 B 物联网业务中使用。由于不同物联网业务功能需求和资费存在差异，物联卡存在被非法使用和套利的风险。
- ✧ 违规滥用：某客户购买卡后，将卡应用于非物联网业务。由于一些物联卡具备短信和语音功能，滥用后可能被用于拨打骚扰电话、发送垃圾短信、通讯信息诈骗等。
- ✧ 其它违规情况：大量的机卡分离、换卡等行为，这些物联卡可能被安装在猫池中进行薅羊毛，或者存在被用来进行电信诈骗、违规上网等风险。

二. 绿盟科技物联网安全风控平台

2.1 产品概述

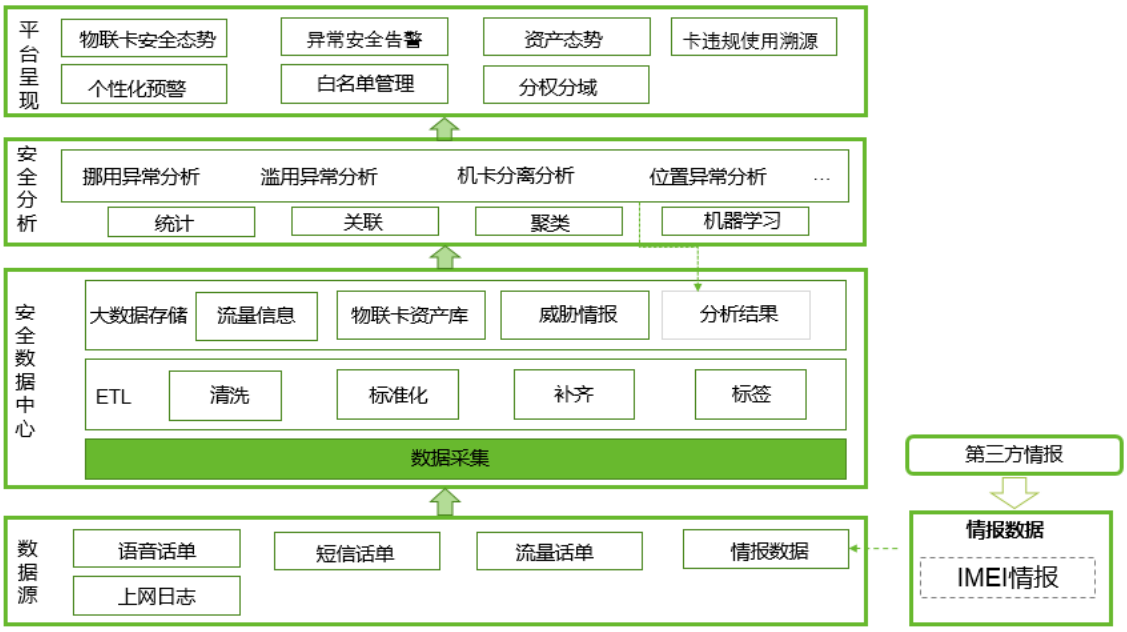
目前大量物联卡用于物联网业务，面向电力、金融、交通等行业。由于大量物联网终端在用户侧，难以落实安全管理要求。根据 2017 年的两部委考核细则，工信部针对物联卡业务提出了明确的管理要求，包括：

- ✧ 未按要求对物联卡进行实名登记，每发现一张扣 5 分。
- ✧ 电信企业未对物联卡功能、业务范围、使用场景等进行严格限定和绑定，致使可使用合同约定外的业务和功能的，每发现一张扣 5 分。
- ✧ 电信企业未对物联卡使用情况进行有效监测及处置，致使卡被二次销售或挪作他用的，每发现一张扣 5 分。

绿盟物联网安全风控平台针对物联卡业务安全问题，很好地满足了运营商客户的合规要求。通过收集语音话单、短信话单、流量话单、上网日志等物联网卡相关数据，进行数据整合，特征提取，利用大数据分析技术，形成物联卡异常分析模型。针对不同的业务场景，物联网安全风控平台帮助企业发现和定位异常卡信息，持续监控物联卡异常行为，提前告知预警，帮助企业部门快速监管核查异常卡，并及时处理，为运营商客户提供物联卡业务安全分析能力，以及对物联卡的合规处置提供决策依据。

2.2 产品架构

绿盟物联网安全风控平台整体架构分为四层，最底层是平台接入的各类数据源，数据主要来源为物联卡的语音话单、短信话单、流量话单、上网日志数据，以及外部情报数据；安全数据中心主要完成原始数据的接入，对数据进行初步的整理工作，包括清洗、标准化、数据补齐、标签化等，以及对数据进行存储，为上层安全分析提供数据支撑；安全分析层负责对数据进行分析，包括统计分析、机器学习等，实现对物联卡的业务异常分析，形成物联卡异常分析模型；平台通过用户视角，将物联卡异常态势进行可视化呈现，包含物联卡安全态势、异常安全告警、个性化预警、白名单管理等功能。



图表 1 绿盟物联网安全风控平台架构示意图

2.3 产品优势

2.3.1 大数据分析技术

安全从业者早已知道，在海量的安全数据中，各类数据之间有千丝万缕的联系，通过对这些联系的分析，可以发现很多靠传统手段无法发现的安全问题。但是面对海量物联卡产生的海量语音话单、短信话单、流量话单、上网日志，传统的利用数据库进行安全分析、数据挖掘变得极端困难。

绿盟科技利用在大数据分析方面的技术积累，形成了安全大数据分析技术。二者结合提出了多种物联卡业务分析特征，将以往不可能的安全大数据分析变为可能。

2.3.2 超强物联卡安全分析模型

物联卡在资费方面存在流量池计费、无漫游、资费较优惠等特点，在销售给客户后存在挪用异常、滥用异常和其他异常等安全风险。如何分析出物联卡的安全风险，对物联卡进行有效监管是一个难题。

绿盟科技经过多年的研究，在物联卡的安全分析上积累了大量经验，提出了多种安全分析模型，可以有效发现物联卡的挪用、滥用、其它异常等安全问题。多个安全模型的配合使

用，可以从多个维度分析物联网的安全问题，并从准确率和查全率上双向保障物联卡的检测效果。

2.3.3 情报关联分析

绿盟科技经过多年的研究，在 IMEI 上积累了大量的情报。借助于 IMEI 情报，可以大幅度提高物联卡安全分析的准确性，为物联卡异常的溯源取证提供了极大的便利。

2.3.4 插件化设计

绿盟物联网安全风控平台采用上层业务模块插件化处理，使业务模块与平台功能实现一对一设计，业务模块的新增和优化便不会影响其他模块或平台功能，将业务模块抽象化并与平台功能实现分离，从而提高研发效率，降低企业维护成本。

2.4 主要功能

2.4.1 物联卡异常检测

物联卡违规使用往往是物联卡没有按照合同规定应用到对应的物联网设备类型中，将物联用到其他物联网领域或者非物联网业务，用于个人使用。由于不同物联网业务资费存在差异，物联卡挪用将导致非法套利的风险；另一方面，具备短信、语音功能的物联卡，存在被用于拨打骚扰电话、发送垃圾短信、通信诈骗等风险，物联卡的频繁换卡、机卡分离，将存在薅羊毛、非法上网等风险，可能导致公司经济损失。

绿盟物联网安全风控平台可以通过流量、短信、通信频率、通信时长等多个维度进行安全检测分析，判断物联卡是否出现挪用、滥用等违规行为，并给客户呈现异常卡信息以及用卡单位和发卡单位信息，帮助客户在监管部门审查前能够提前告知预警，并及时对异常物联卡进行处置。

2.4.2 白名单管理

针对特殊业务的物联卡或者用卡单位，正常情况下会被系统检测出物联卡违规使用，产生告警日志，面对这种场景，绿盟物联网安全风控平台可以提供白名单管理功能，将这些无风险的卡号或者业务部门制定成白名单，在进行异常卡检测时，可针对性过滤白名单中的卡数据内容，不做异常检测分析，帮助用户在进行异常卡核查时减少核实工作。

2.4.3 个性化预警

物联卡广泛应用于电力、金融、交通、环境监控等行业，针对不同的业务场景，需要分析的设备特性也不同。

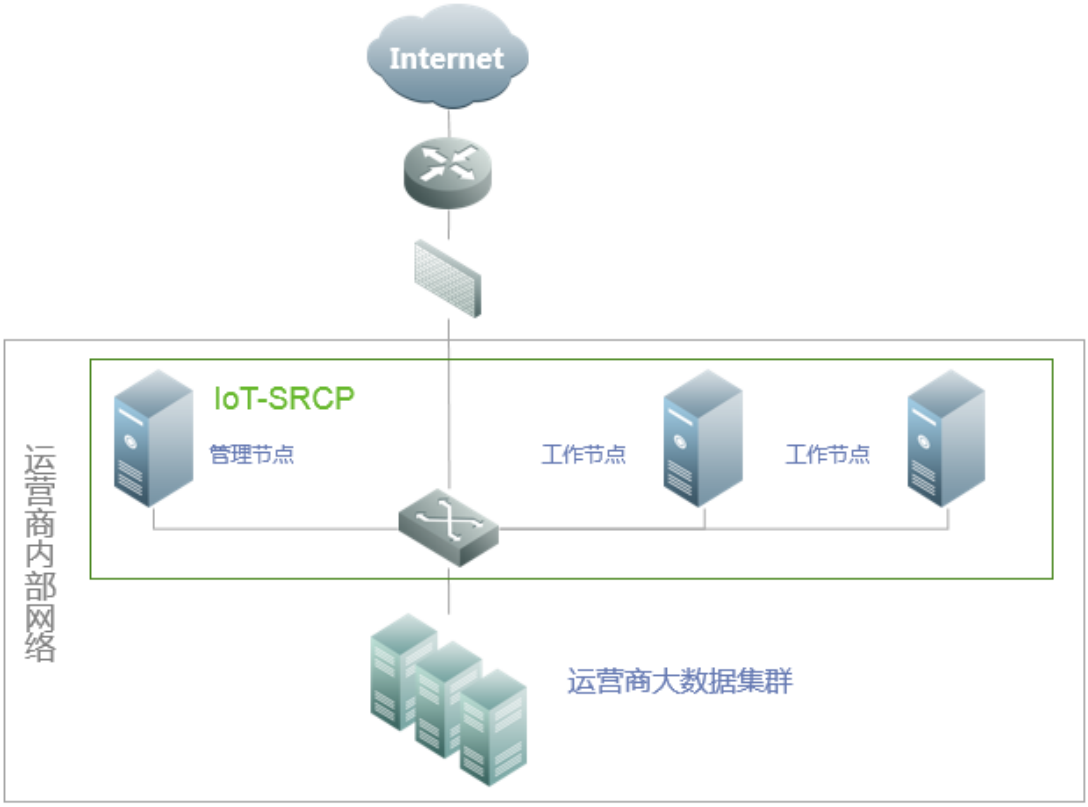
绿盟物联网安全风控平台提供个性化预警功能，客户可以通过自定义制定预警策略，对物联卡的语音、短信、流量行为以及其他信息进行预警。根据不同的配置，进行个性化预警分析，检测异常事件，提供检测、查看针对性范围预警事件的能力，其中包含被叫范围、设备 IMEI 号、使用位置、服务器地址等信息，以便实时掌握物联卡状态，及时了解预警事件并进行处理。

2.4.4 历史行为轨迹

针对系统已检测出违规行为的异常物联卡，绿盟物联网安全风控平台提供历史行为轨迹功能，支持查看异常卡过去一段时间内的语音、短信、流量和上网日志等行为信息，在处置审核物联卡时，成为物联卡取证、溯源分析的重要方式。平台通过关联分析，建立物联卡的行为轨迹，支持对挪用、滥用、其它异常中的各种异常物联卡历史行为轨迹的查看。

2.5 典型部署

物联网安全风控平台由多台高性能服务器组成集群，部署在客户内网中，可同时提供数据接入、数据分析、数据查询、可视化呈现等功能。运营商的卡信息、语音话单信息、短信话单信息、流量话单信息、上网日志信息等数据会实时传输到运营商大数据中心，运营商大数据中心再将数据通过内网传输到物联网安全风控平台。



图表 2 绿盟物联网安全风控平台部署方式

三. 客户利益

3.1 满足工信部考核要求

- 满足工信部 452 号文提出的抓紧完成企业侧技术手段建设，提升企业侧技术防范打击能力；
- 2019 年部委考核：加强技术手段建设，做好物联网行业卡使用监测管理
- 提前告知预警，避免出现违规事件，被监管部门扣分，被集团通报批评。

3.2 为信安部门提供检查监督工具

- 发现和定位异常物联卡，可以为业务部门客户提供接口查询客户经理、合作企业是否有违规历史，提前知晓合作企业的信誉度；
- 提供物联卡业务运营和监控手段，帮助客户了解当前物联卡整体的状态，异常卡趋势，重点分布的单位，及时进行审核处理。

3.3 为集团客户经理提供决策支持

- 签约销售前，为客户经理提供企业资质和信誉评估的参考依据，查看合作企业是否有劣迹行为，信誉如何；
- 签约销售后，提供物联卡和用卡单位的持续监控，对合作企业提供数据支撑，帮助用户快速审核，提高运维效率。