金融风控下的
终端应用风险监控

梆梆安全

梆梆安全　　赵千里

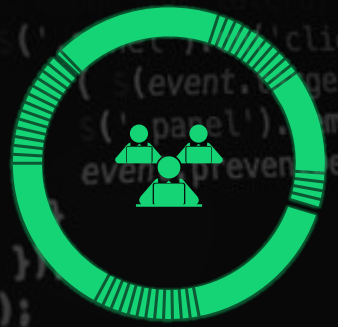
REC

C O N T E N T

目 录

PART ONE

移动金融安全建设现状



PART TWO

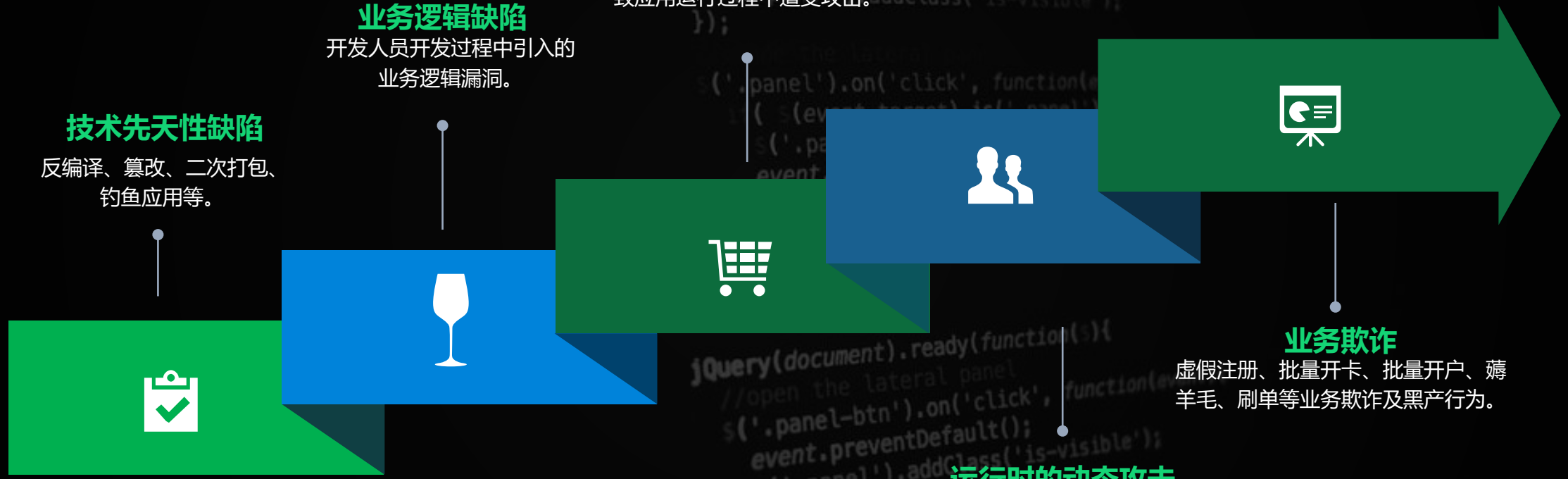
新的挑战与威胁

PART THREE

终端应用风险监控

00:00:01.706

移动安全威胁的演进



技术先天性缺陷

反编译、篡改、二次打包、钓鱼应用等。

业务逻辑缺陷

开发人员开发过程中引入的业务逻辑漏洞。

操作系统漏洞

操作系统底层的安全机制不健全，导致应用运行过程中遭受攻击。

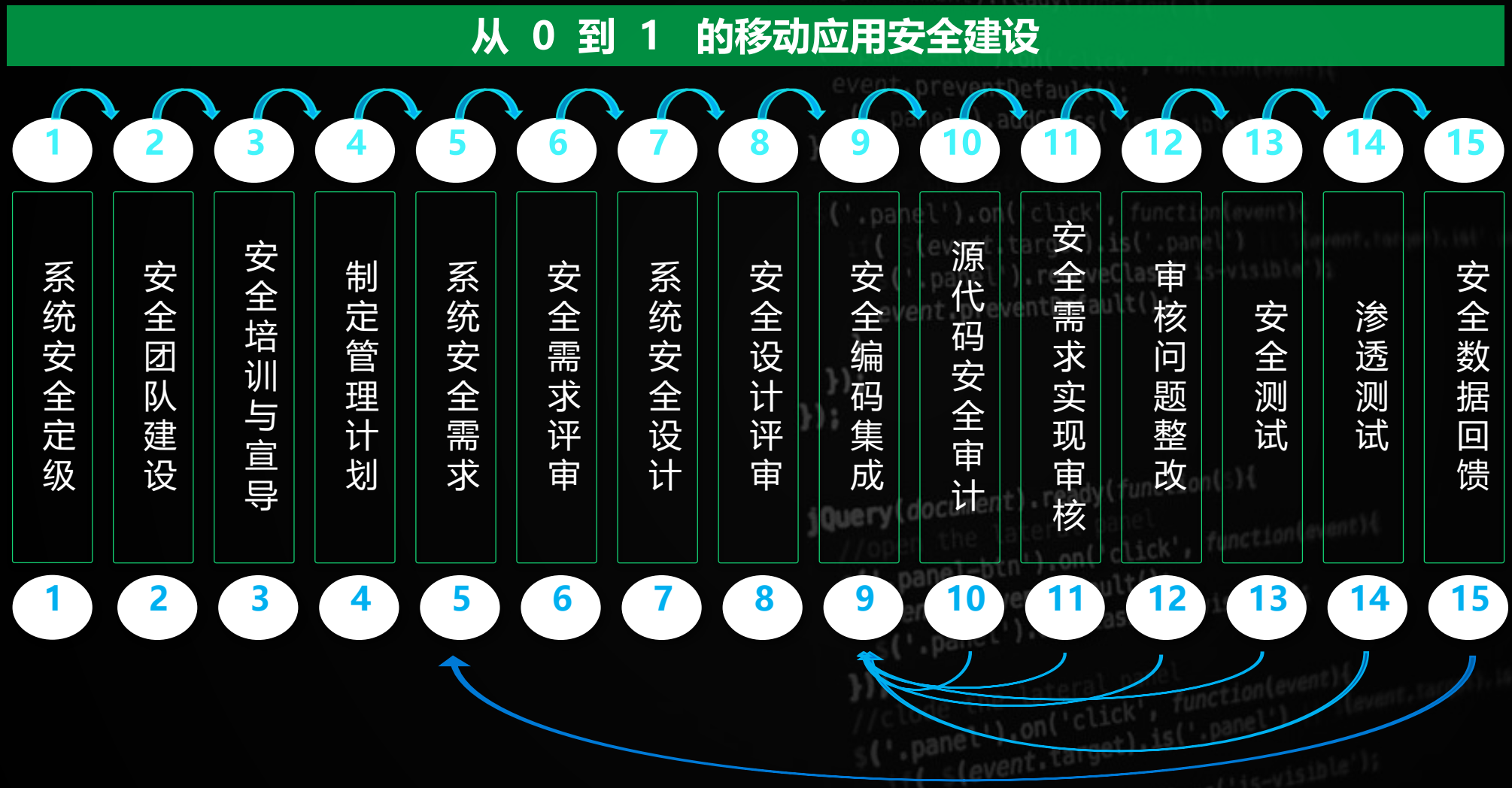
运行时的动态攻击

模拟器、注入攻击、调试行为、设备篡改、位置欺诈等运行时的动态攻击。

业务欺诈

虚假注册、批量开卡、批量开户、薅羊毛、刷单等业务欺诈及黑产行为。

移动安全建设从0到1



在过去的五年中，绝大多的金融企业实现了移动安全的从0到1。我们协助部分的金融企业完成了SDLC的安全体系流程的建设与落地，利用技术化的手段保证管理制度的落地执行。

发布之前做渗透测试、源代码审计、安全加固基本已经成为所有金融企业的必选安全手段。

业务安全威胁的加剧

保障账户安全

- 防撞库——防止利用已泄露的用户名口令进行批量登录，尝试获取可登录账号。
- 防虚假注册——防止利用自动脚本批量注册大量垃圾账号。
- 防短信轰炸——防止黑客滥用短信发送接口，批量或向指定手机号发送垃圾短信，影响正常手机使用。
- 防批量开户——防止攻击者通过自动化工具批量开户，造成用于薅羊毛、洗钱等不法行为。
- 防批量办卡——防止攻击者通过自动化工具批量申请信用卡、银行卡等，造成虚假信用卡、银行卡，造成经济损失。

防范业务欺诈风险

- 防刷单——防止通过自动化工具批量实现业务交易，从而获取不正当利益。
- 防套现——防止恶意用户通过技术手段绕过限制，利用虚假交易换取网站积分，兑换礼品后套现获利。
- 防交易篡改——防止攻击者通过中间人攻击等行为，进行交易篡改。
- 防线上盗刷——防止攻击者通过撞库等方式获取用户信息，盗刷用户银行卡、积分等。
- 防有价积分盗用——防止攻击者利用自动化工具，获取用户账号信息，批量盗取和消费用户商城或信用卡的积分。

防止数据泄露风险

- 防爬虫——防止爬虫爬取个人信息以及客户保单、账单等金融产品信息。
- 防账户数据遍历——防止利用漏洞或者合法身份，通过工具批量查询导出客户资料。
- 防零日攻击——防止利用web零日漏洞的各种自动化攻击。
- 防扫描——防止黑客通过漏扫工具扫描网站结构和漏洞。

黑产盛行成为金融主要对抗对象

百万黑产
从业者

千亿资金
规模

近几年移动互联网的普及，导致移动终端成本的不断降低。同时为了获取新用户，银行在直销银行等业务推广过程中投入资金给予新用户优惠。然而大量优惠缺未到真正用户端，地下黑产从业者紧盯银行羊毛，利用模拟器甚至真机以正常身份注册进入，批量刷票刷单薅羊毛，获取暴利，据《中国移动互联网发展状况及其安全报告（2017）》显示，截止2016年底，中国拥有23亿活跃移动终端，移动互联网网民才6.95亿，由此可见一斑。

业务安全防御手段正在面临挑战

设备绑定规则

通过终端设备信息造假，令后端业务风控系统误认为前端是新设备。

位置信息造假

通过GPS坐标篡改，让后端业务误认为用户还在常规使用地点。

业务规则绕过

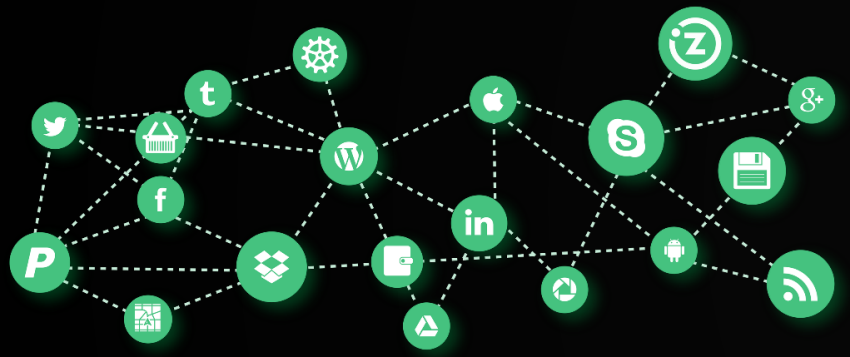
通过在前端Hook系统接口，让本应该通过拍照上传身份证的验证方式可以传一张本地已存照片。

业务风控/反欺诈频繁失效

在过去的5年中，绝大部分的企业已经建立了基于规则、模型的业务风控/反欺诈系统等业务安全防护类系统，用于抵御黑产、薅羊毛等业务安全问题。

然而，业务安全防护类系统是一个偏重于后端的系统，通过收集前端的设备、系统、行为、交易数据，通过规则和模型判断交易的异常情况。事实证明，在缺乏前端安全监控与防御的情况下，前端数据造假已经成功欺骗后端业务安全系统。

风控基本结构



数据采集

数据处理、存储

数据分析、决策

终端设备信息造假

通过**终端设备信息造假**，令后端业务风控系统误认为前端是新设备。

[终端设备信息造假DEMO]

终端位置信息造假

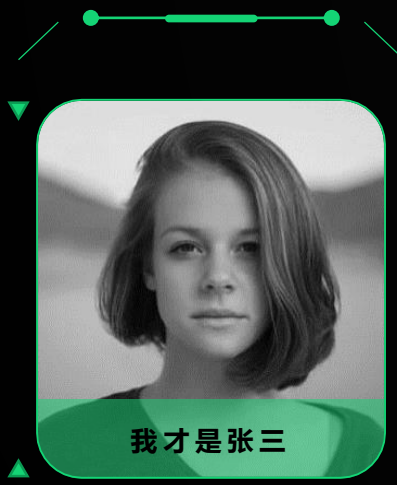
GPS坐标篡改

GPS坐标篡改DEMO

终端图片信息造假

身份验证图片替换

终端数据造假造成风控决策系统效能下降



数据采集

数据分析、决策

终端应用运行时风险概览

终端设备不可信

终端应用可能运行在模拟器、设备信息造假等非可信设备上。

运行环境不可信

终端应用可能运行在存在病毒木马的非可行操作系统上，应用安装包为非官方发布合法安装包。

操作手段不可信

终端用户可能存在隐藏真实地理位置，对应用进行批量机器操作等非正常的使用手段。

本地逻辑不可信

终端黑客可能使用注入、调试等多种手段绕过本地的业务控制逻辑。

梆梆安全移动威胁感知平台

感知 **阻断** **溯源**

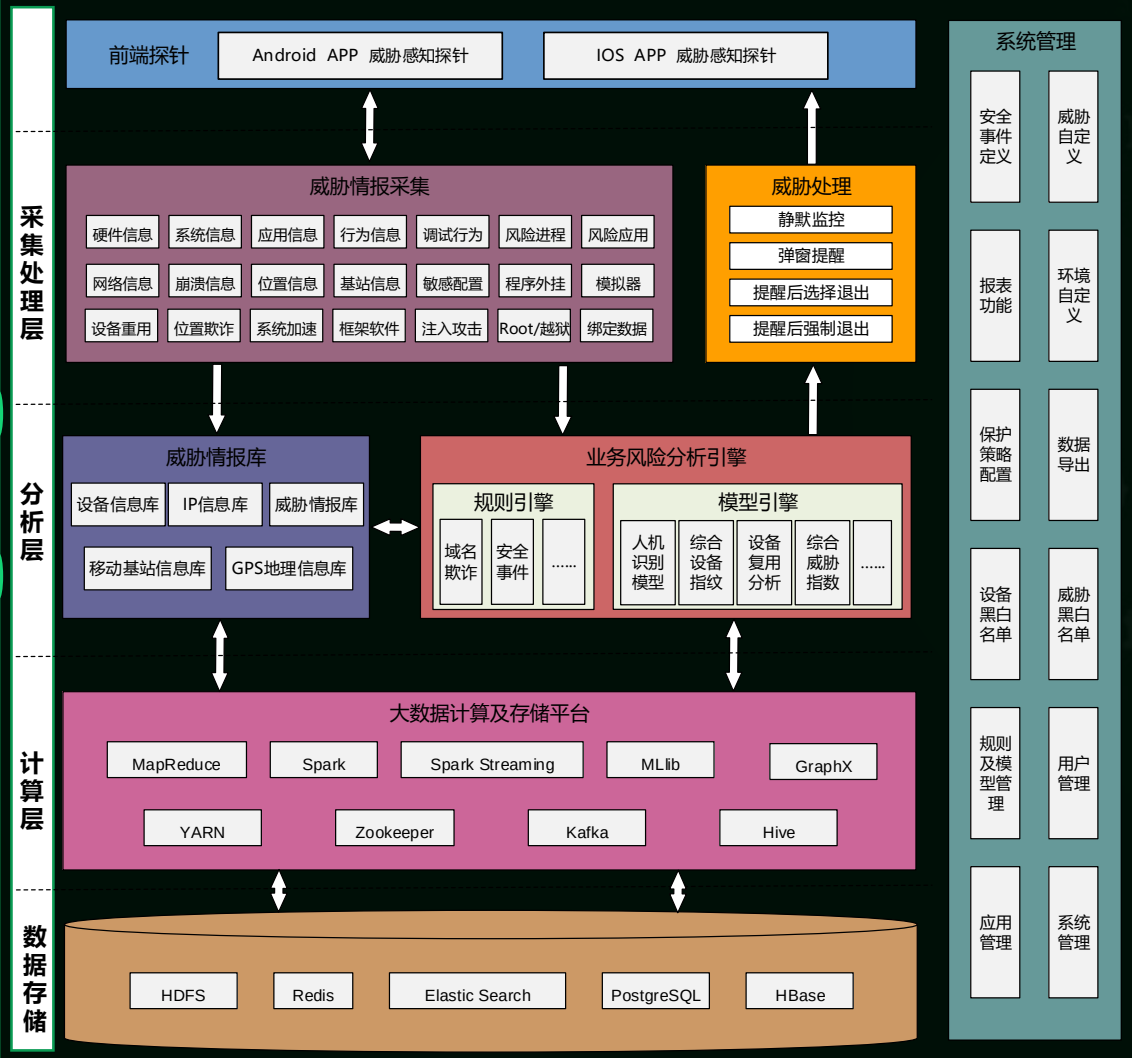
通过在移动应用中植入威胁感知探针，在应用运行过程中，威胁感知探针犹如保镖一样监控应用运行状态，从技术攻击的源头发现各类异常违规操作，阻断并且采集攻击特征，以达到感知、阻断、溯源的目的。

移动应用的贴身保镖

梆梆安全的移动威胁感知平台从代码安全的本质出发，站在主动防御的角度，为每个用户在使用应用的过程中配备贴身保镖。

移动终端威胁感知

平台架构设计



梆梆安全移动威胁感知平台通过对移动客户端运行时大量系统底层数据及威胁数据的采集、处理及关联分析，从而实现对当前移动客户端运行环境可信和安全状况的主动监测。平台从前往后主要分为前端SDK探针、采集处理层、分析层、计算层、数据存储层。整体平台的底层依托于hadoop、spark的大数据计算平台，为所有数据采集、处理、分析提供基础的计算资源，从而保证所有业务分析的实时性和可靠性。

移动终端威胁感知


椰椰安全 | 移动威胁感知
综合态势
威胁态势
运行分析
崩溃分析
报表功能
策略配置
系统配置
中文
安全事件统计
安全事件总数
事件设备总数
威胁分类统计
启动趋势
崩溃趋势
2018-10-15
2018-10-24

威胁详情
威胁名称
注入类别
分析结果
威胁说明
UDID: 7662b5bd-de51-350e-8f85-ea6aab2a71e3
时间 2018-11-14 / 2018-11-14
安全事件
威胁分析
环境安全
运行分析
崩溃分析
设备信息
安装应用信息
框架软件
最近异常时间
异常分析
2018-11-14 12:50:22
系统安装有框架软件: Xposed Installer， Cydia Substrate， busybox
异常说明: Xposed、Cydia Substrate及Frida等框架软件是攻击者在运行过程中进行注入、Hook等攻击的常用工具，框架软件的安装和使用会对正常应用的使用造成极大安全风险。
Root/越狱
最近异常时间
异常分析
2018-11-14 12:50:22
系统Root
异常说明: Root/越狱被广泛运用于使用者想获取系统最高管理员权限，已达到卸载预制应用、安装非授权应用等场景。Root/越狱后的手机安全强度极低，当恶意程序获取系统权限后，可以监听用户隐私，窃取敏感资料，会大大降低手机安全性。

移动终端威胁感知-安全威胁

威胁检测点

应用破解、模拟器、位置欺诈、域名欺诈、设备复用、注入攻击、调试行为、程序外挂、系统加速。

威胁统计

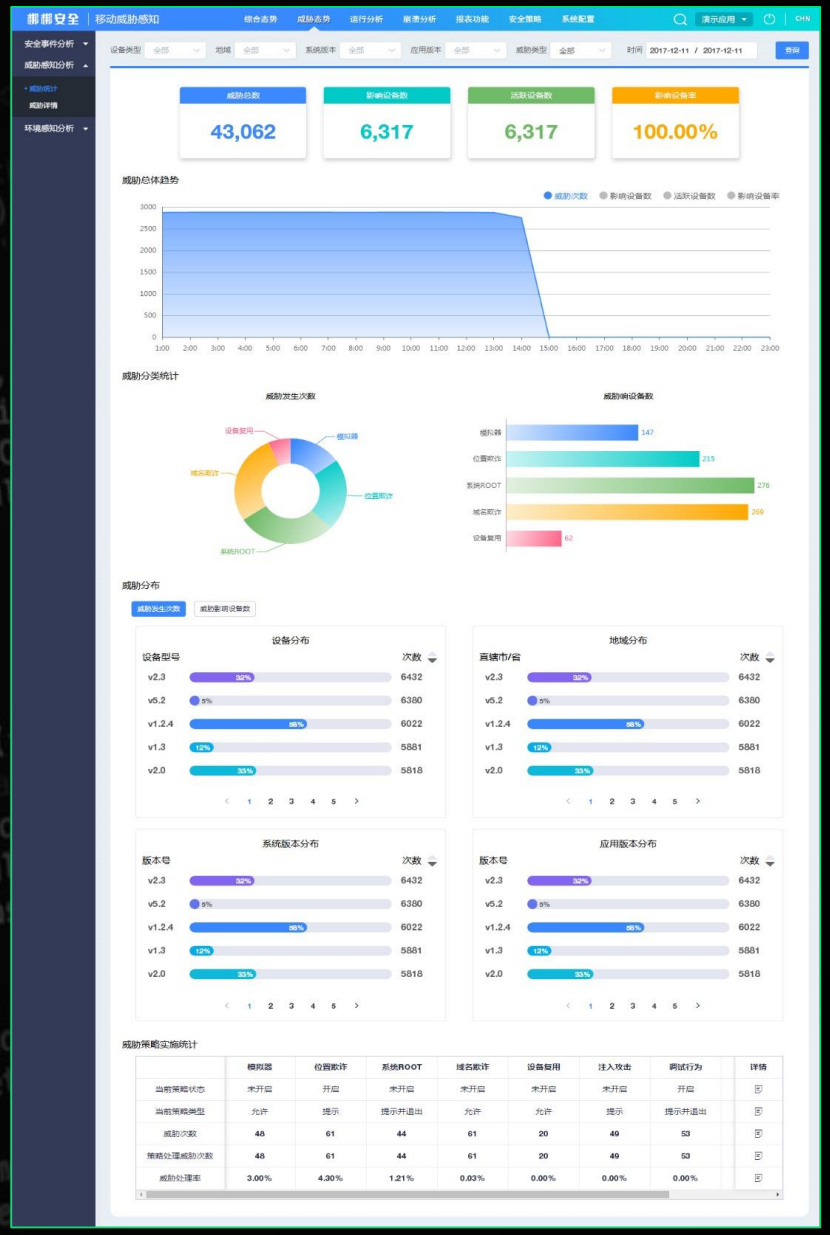
从设备类型、地域、系统版本、应用版本、时间等维度对威胁进行筛选统计，查看威胁总数，威胁影响设备数，活跃设备数，影响设备率，查看其总体趋势，威胁发生次数，威胁影响设备数，威胁分布及威胁策略实施情况。

威胁详情

从设备类型、地域、系统版本、应用版本、时间，威胁类型等维度对威胁进行筛选统计，对威胁进行地域、设备、系统、应用排行。支持威胁总数和威胁设备进行详细查询，详细信息包含威胁发生时应用设备信息，应用信息等。

威胁攻击链

针对单个设备的威胁事件提供攻击链展现和分析，可以明晰看到单个设备历史的安全威胁发生状况，可以利用攻击链行为进行事后攻击追溯。



移动终端威胁感知–环境风险

环境检测点

Root/越狱、框架软件、风险应用、风险进程、敏感配置。

环境统计

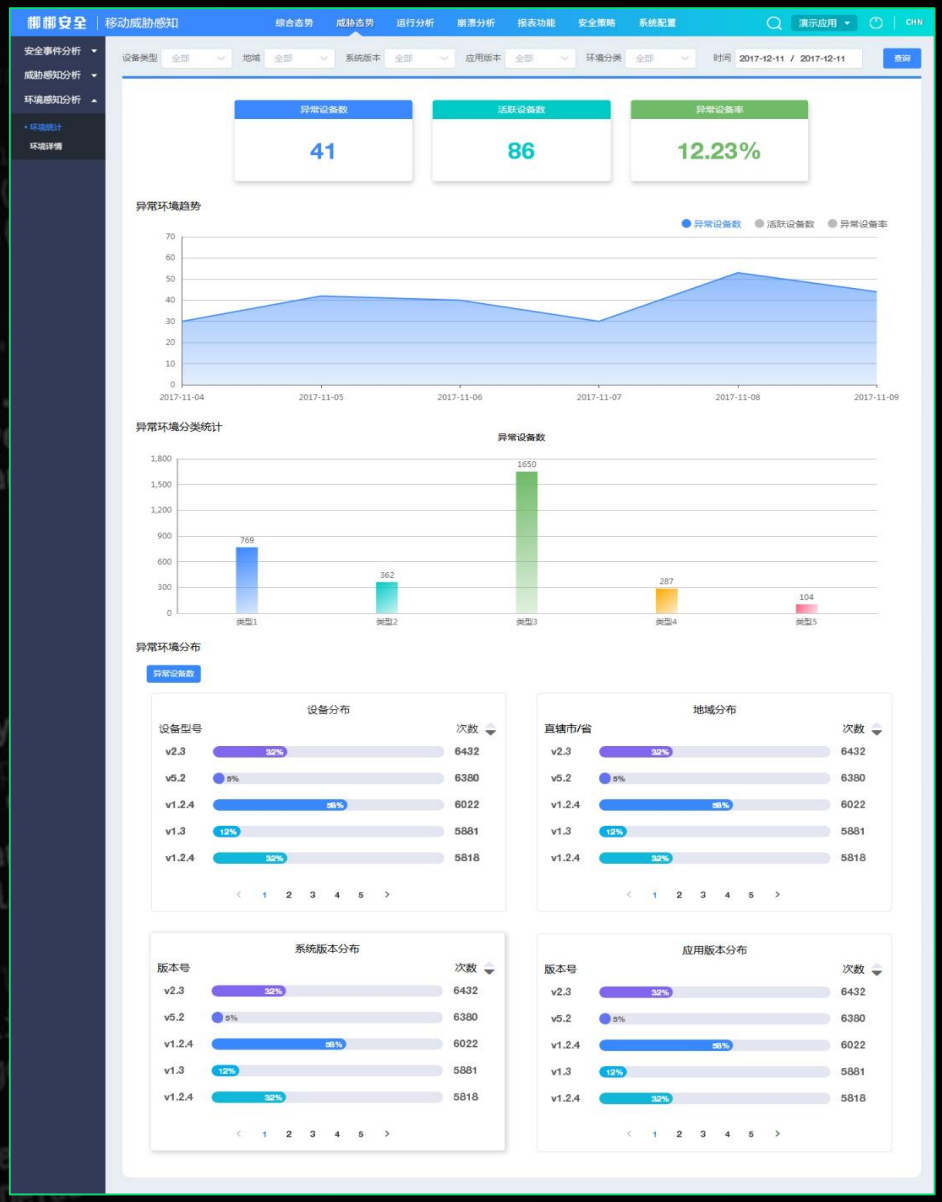
从设备类型、地域、系统版本、应用版本、时间等维度对环境风险进行筛选统计，查看环境风险影响设备数，活跃设备数，影响设备率，查看其总体趋势，环境风险发生次数，环境风险影响设备数，环境风险分布。

环境详情

从设备类型、地域、系统版本、应用版本、时间，环境风险类型等维度对环境风险进行筛选统计，对环境风险进行地域、设备、系统、应用排行。支持环境风险总数和环境风险设备进行详细查询，详细信息包含环境风险发生时应用设备信息，应用信息等。

环境攻击链

针对单个设备的环境风险事件提供环境异常统计展现和分析，可以明晰看到单个设备历史的环境风险发生状况，进行事后攻击追溯。



技术与理念的创新

01. 主动防御战线的前移

通过梆梆的移动威胁感知平台能够将企业的主动安全防御能力前移，能够尽早发现可疑行为和恶意攻击。

02. 从技术源头的防御

移动威胁感知平台实现了防御理念的创新，从攻击技术的源头识别和检测各类攻击，不需要借助于业务交易数据。

03. 移动端的态势感知

移动威胁感知的推出是移动端的态势感知平台，真正的实现了事前威胁感知的能力，从防御“坏事”到识别“坏人”的转变。

自适应移动安全PPDR防御体系

3

通过威胁情报，预先发现新的攻击

4

实现更有针对性、有效的防御体系

2

迅速理解问题原因和影响，并作出响应

1

发现穿透现有防御系统的高级攻击

中国某国有银行

项目名称

终端操作风险监控项目

客户业务场景

中国某国有银行建设有完善的业务风控系统，手机银行用户量2.6亿。手机银行在发布后，第三方机构对手机银行进行渗透测试，并且对外发布手机安全评估报告，直到报告公布之前，该行对此毫不知情。由此，凸显出来对应用发布后，来自客户端的各种攻击、渗透测试行为等没有监测和预警能力。

客户痛点及需求

对于终端操作风险进行监控：重点包括注入、调试等黑客攻击行为，包含位置篡改、设备信息篡改、模拟器、猫池等异常操作行为。能够针对单个安全威胁定制在时间、频次两个维度定义安全事件，对安全事件进行重点监控。

二期及后续需求

加入物联网、外发SDK的终端操作风险监控；
将终端操作风险监控的威胁情报上送业务风控系统
根据用户终端操作风险进行认证方式的智能化选择
做差异化智能认证体系

四川某银行

项目名称

手机银行安全监控与运行监测项目

A

客户业务场景

客户的手机银行作为行方的重要业务渠道，且每年的用户呈现明显增长趋势，在IT科技建设处于区域领先水平，全行建设有业务风控系统，但未做到客户端的实时监控。2016年，人民银行发布《170号文件》和《192号文件》，目前行内系统无法达到文件要求的客户端风险监控。

B

客户痛点及需求

满足监管要求；
能够检测交易终端的环境安全风险；
能够发现客户端攻击行为；
对于监测到的攻击行为能够及时反馈后台，并且能够实时阻断；监测到的安全威胁数据能够反馈业务风控系统；能够有一个实时监测滚动的大屏，展现客户端的攻击事件；

C

二期及后续需求

利用大数据平台，在现有的运行分析基础上，做业务运营分析。
将威胁感知的威胁情报上送业务风控系统。

D

客户案例分享

银行业

建设银行
民生银行
贵阳银行
包商银行
天府银行
九台农商
丹东银行
阜新银行
宁夏银行
中关村银行

政府行业

国务院办公厅
福州市政府

互金、保险

玖富万卡
合缘万卡
华润通
蜡笔分期
玖富普惠
中国人保财险

运营商行业

中国移动
中国联通
中国电信

交通行业

首汽约车
知豆汽车
北京公交


THANK YOU!