网络空间威胁对抗防御技术研讨会
暨 第十届安天网络安全冬训营

沧海横流

执行体全量识别与精细管控

移动办公场景的安全解决方案

安天 | 移动安全中心

目 录

01 移动办公安全风险问题

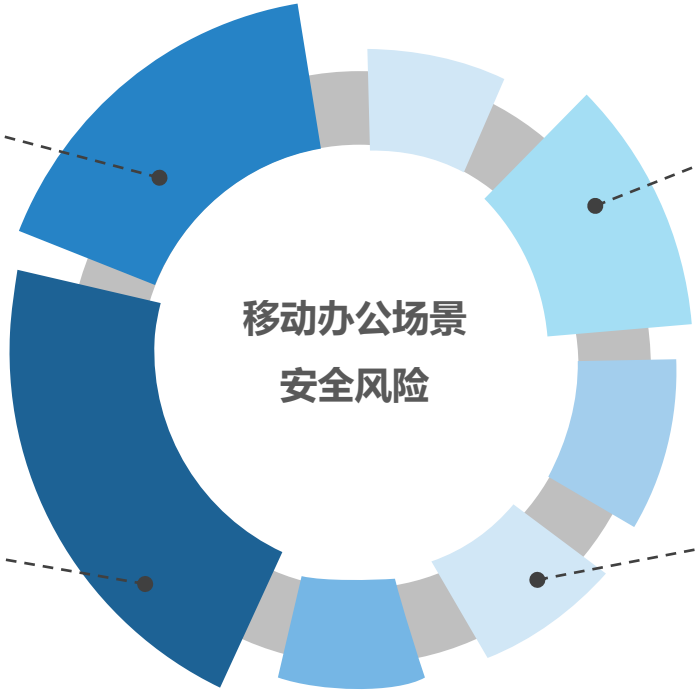
移动办公场景存在诸多安全风险

数据信息泄露风险

- 移动设备托管、借用或丢失，导致数据泄露风险。
- 内部员工泄密：通过截屏发给好友，或直接发送内部文件，或查看工作不相干内部资料。

接入访问安全风险

- 企业使用内网VPN，通过VPN技术接入的设备本身具有不安全性，导致的各种漏洞时有发生，使整个内网都面临风险。



移动应用安全风险

- 移动APP可能存在一些高危漏洞，攻击者可利用这些漏洞窃取用户数据，进行APP仿冒、植入恶意程序、攻击服务等。
- 移动APP可能被劫持、加载、SQL注入、动态调试等攻击。

移动端恶意攻击风险

- 钓鱼邮件、钓鱼短信攻击。
- 利用仿冒应用、木马应用进行攻击。
- WIFI 中间人攻击。

数据信息泄露风险——移动端泄密事件

某保密部门陈某某在有专用保密手机的同事，私自购买 手机，并且在公司使用未经审批的“机外机”，通过微信、QQ等聊天工具，与家人朋友谈论涉密内容、发送涉密照片，并在手游平台暴露其身份，严重危及秘密安全。陈某某被给予严重处分。

移动端会泄密哪些内容？

- 手机号
- 身份证号
- 银行卡号
- 短信验证码
- 手机照片
- 接收的文档
- 聊天记录
- 位置轨迹
- ……

接入访问风险——内网VPN风险

根据云安全公司Zscaler调研报告表明：

截止到2022年10月，**超过95%**的受访企业利用VPN服务进行安全远程访问，高于去年的93%，且CVE（常见漏洞与暴露）数据库中的已知VPN漏洞高达近**500个**。

自从2020年冠状病毒（COVID-19）爆发以来，由于远程办公的必要需求，企业VPN使用量增加了33%，这也成为黑客发起攻击的一个突破口。据相关媒体报道，与韩国有联系的威胁组织利用零日漏洞攻击了某中国政府机构，该漏洞影响了境内VPN服务。数据显示，从3月开始，DarkHotel组织就已经锁定了许多中国机构。据悉，攻击者利用 某互联网企业的VPN服务中一个**安全漏洞来传播后门恶意软件**。黑客利用VPN客户端更新过程中的漏洞，用后门取代了合法的更新，黑客大约攻击了200个VPN服务器并注入恶意软件。

移动应用安全风险——政企应用存在风险问题

1、XX省统计公共移动应用2102个（含新增和原有存量数）其中有超过 **70%** 均存在着不同等级的安全风险；约 **15%** 的应用存在高危风险情况。

2、 XX市公共移动应用507个，约占全省公共移动应用数量的24%。经初步分析评估，XX市约 **20%** 的APP存在高危风险情况。

3、 对XX市涉及政务和民生领域的移动APP分析评估结果表明，约 **15%** 的政务、民生公共领域APP存在高危风险情况。

风险度排名	应用名称	主要问题（高危风险）
5	XX交警	允许程序备份，极易导致个人隐私及敏感信息泄露
6	云上XX	采用http协议进行明文传输，允许随意查看一些通信信息，允许程序备份，十分容易导致信息泄露，如账号信息（电话、邮箱）等
19	XX绿道	采用http协议进行明文传输，并且可随意查看和篡改通信内容，允许程序备份，容易导致运动数据、车牌号、搜索记录等信息泄露
27	XX出入境	采用http协议进行明文传输，允许程序备份，泄漏个人信息（帐号、密码的哈希、身份证号、户籍、联系电话等），且信息可被篡改
43	XX地铁	攻击者可以伪造恶意短信内容发送，散播虚假消息；采用http协议进行明文传输，可被劫持，任意篡改内容

移动端恶意攻击风险——钓鱼、仿冒组合攻击

2021年自春节起，全国多地市连续发生通过群发短信方式，以手机银行失效或过期等为由，诱骗客户点击钓鱼网站链接而盗取资金的安全事件。

据Bleeping Computer网站2022年8月8日消息，云通讯巨头Twilio表示，有攻击者利用短信网络钓鱼攻击窃取了员工凭证，并潜入内部系统泄露了部分客户数据。攻击者冒充公司内部的IT部门人员，向公司员工发送短信，警告他们的系统密码已经过期，需要通过**点击短信附带的URL进行修改**。该URL带有“Twilio”、“Okta”和“SSO”等具有高仿真性的字段，受害员工一旦点击便会跳转到一个克隆的 Twilio 登录页面。

02 移动办公安全解决方案

数据信息泄露保护——解决内部数据泄密风险

通过最小化权限管理，结合防截屏、数字水印、文档不落地、内容敏感判定等安全技术，同时利用机器学习对用户行为进行动态识别，判定风险并及时下发处置策略，保障企业数据资产安全。

身份安全

- 基于多因子智能统一身份认证及单点登录，在员工访问内网时每次校验员工身份。

文档安全

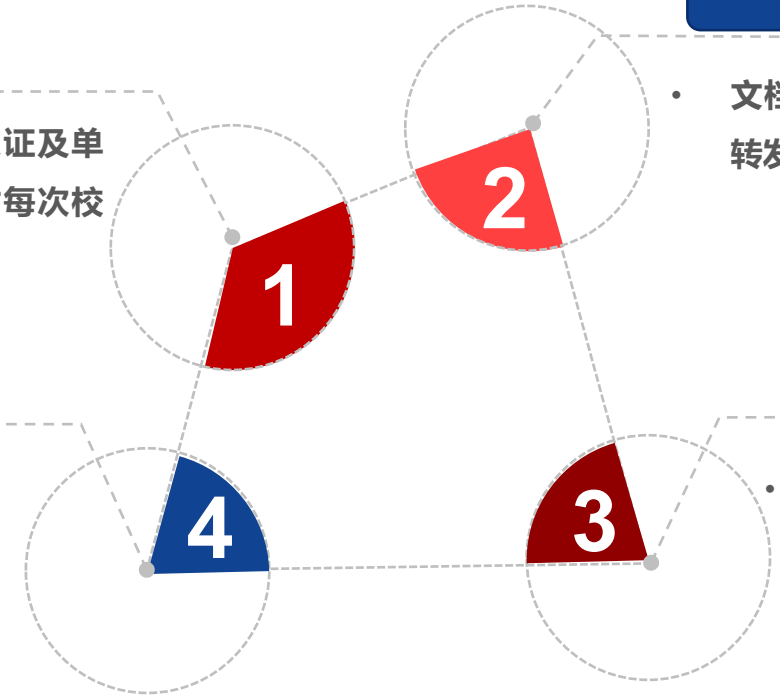
- 文档不落地预览，文档加密，文档水印，转发授权流程，专用安全文档查看器。

行为安全

- 利用机器学习对用户终端环境、用户网络环境、用户访问情况、用户行为习惯等进行判定，及时发现间谍员工。

数据安全

- 链路透明加解密，防截屏，数字水印，数据安全浏览，敏感文档和图片智能识别，白盒密钥。



边缘接入网络保护——解决接入访问安全风险

通过应用安全交付网关，取代传统VPN，实现对内网资源细粒度访问控制，每次访问行为都基于用户身份确认。

- 去边界化安全架构
- 最小授权策略
- 网络隐身
- WAF
- 统一访问入口

终端环境安全检查——解决移动端恶意攻击风险

01 应用检测

- 间谍应用检测
- 隐私窃取检测
- 木马病毒检测
- 风险应用检测

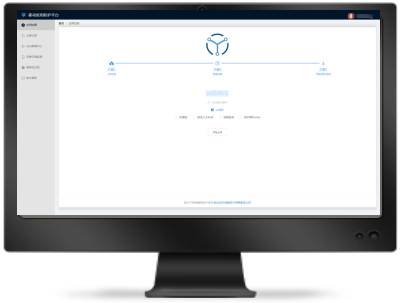
02 URL检测

- 钓鱼短信检测
- 恶意网站检测

03 WIFI检测

- 中间人攻击检测
- WIFI欺骗检测

移动应用安全防护——防范移动应用的安全风险



✓ 安卓应用全面加固

通过对代码、资源文件、配置文件等全方位进行加固，实现各组件协同保护应用安全。

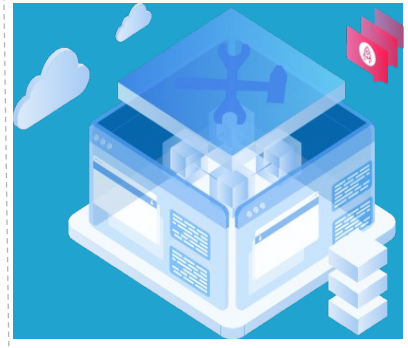
✓ 应用安全生态

提供应用全生命周期的安全防护方案，从测试到加固，协调配合，全面保障应用安全。

为企业提供全面的移动应用加固，防止移动应用在发布到市场后，遭受反编译、调试、盗版、二次打包等威胁。

防篡改

对应用进行完整性校验和签名校验，防止应用被篡改或二次打包。

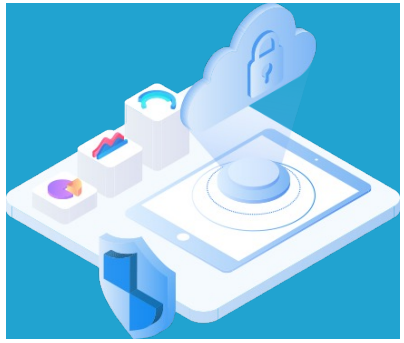


反逆向

对应用进行加壳和代码混淆，防止其被攻击者逆向分析或恢复真实的代码逻辑。

防窃取

对内存数据进行转换和动态跟踪，有效防止数据采集和修改。



反调试

防止攻击者对应用进行动态调试、代码注入，从而有效避免钓鱼攻击、交易劫持、内存数据篡改等恶意行为。

零信任应用安全交付方案

系统基于“端”、“管”、“云”的体系架构，结合移动反病毒技术、应用隔离技术、软件定义边界技术以及身份信任持续评估技术，面向移动以及云计算等新业务场景输出安全防护解决方案。

移动终端安全工作空间（端）

- 通过多因子身份认证、反病毒引擎、应用沙箱为企业提供应用安全工作平台。

移动安全边界（管）

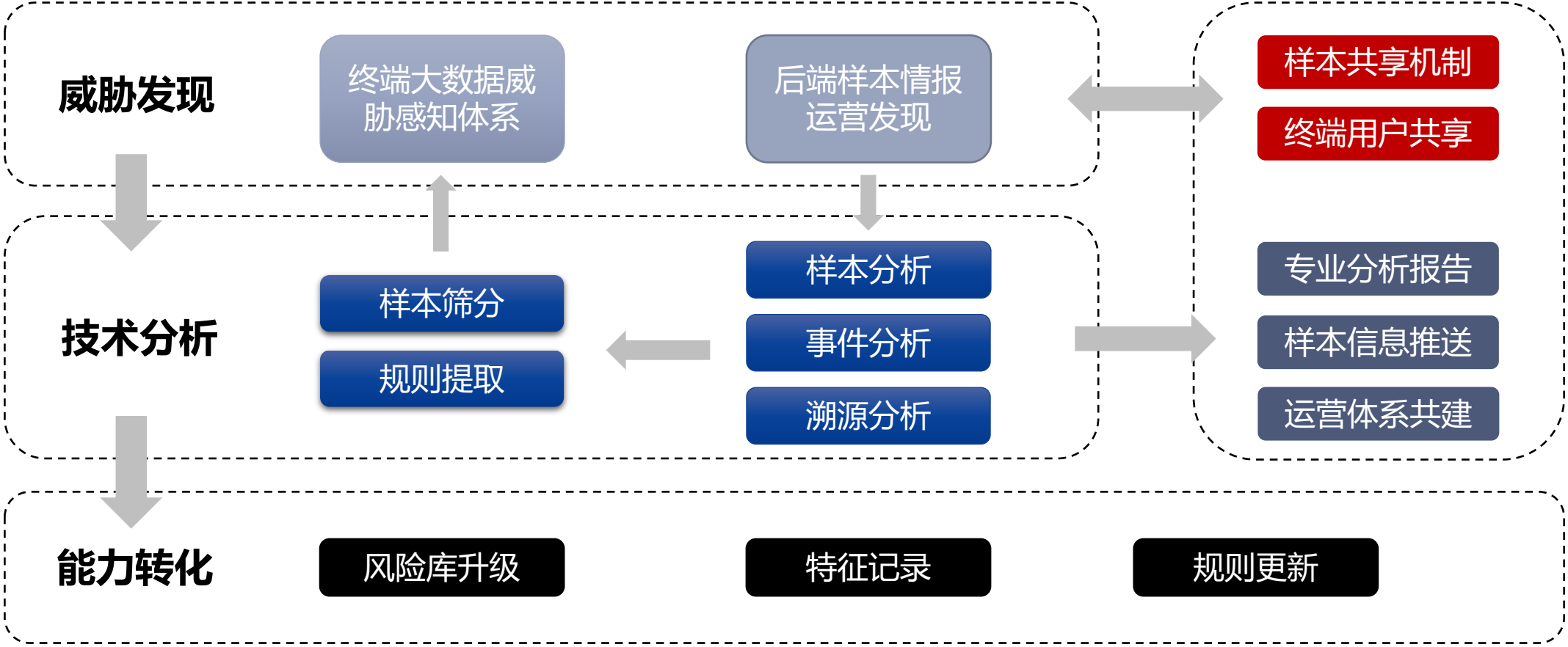
- 通过应用访问代理、身份认证以及权限管控提供统一访问门户，支持访问行为监测，实现边界防护。

移动业务场景安全策略平台（云）

- 从端点设备、用户身份、端点环境、安全基线、端点设备及应用访问行为等多个维度，分析并发现异常及风险，通过身份、状态、行为、内容的持续信任评估策略，为用户提供动态访问控制

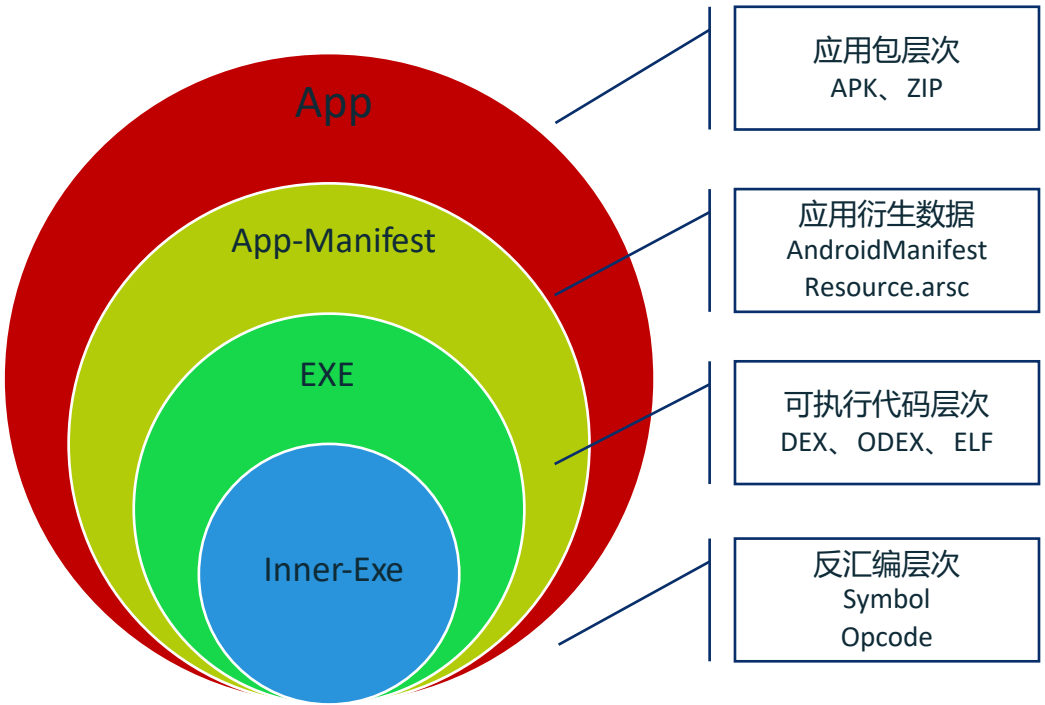
03 移动安全风险运营能力

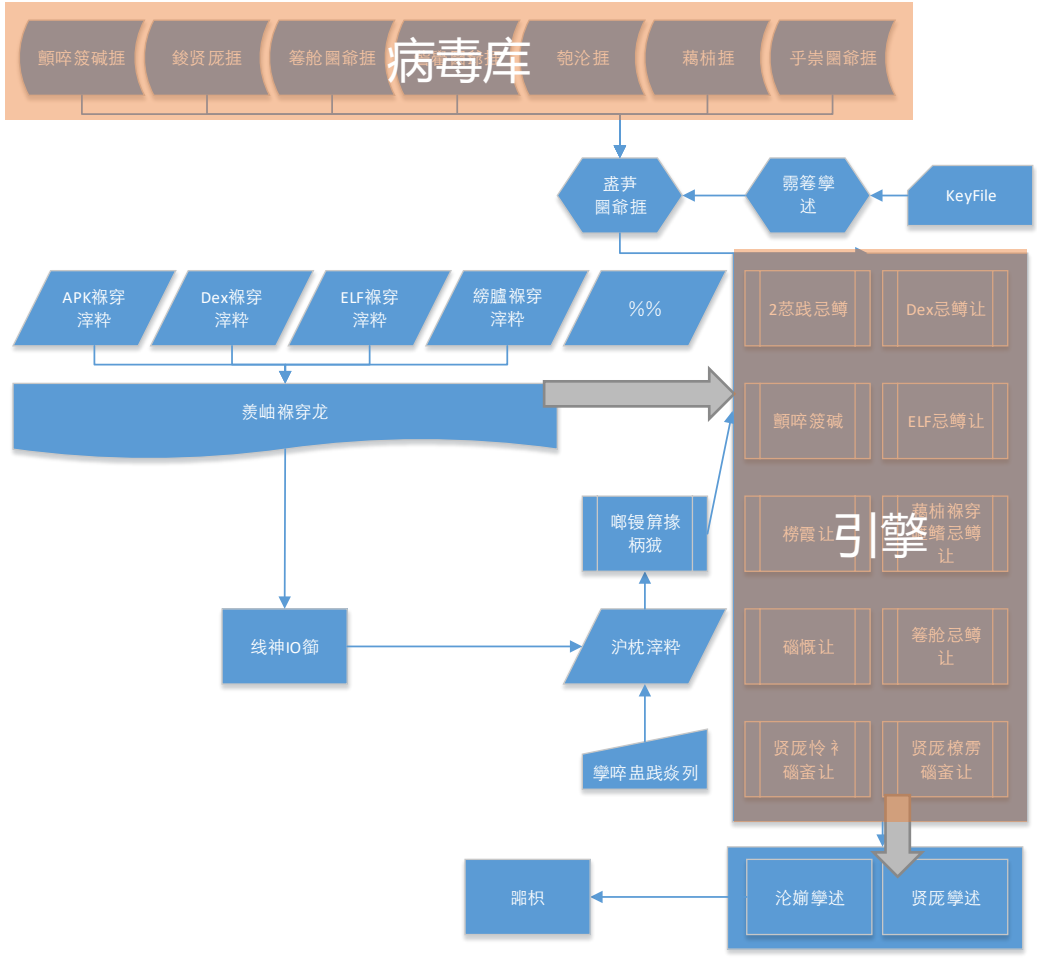
移动办公场景应用威胁采集



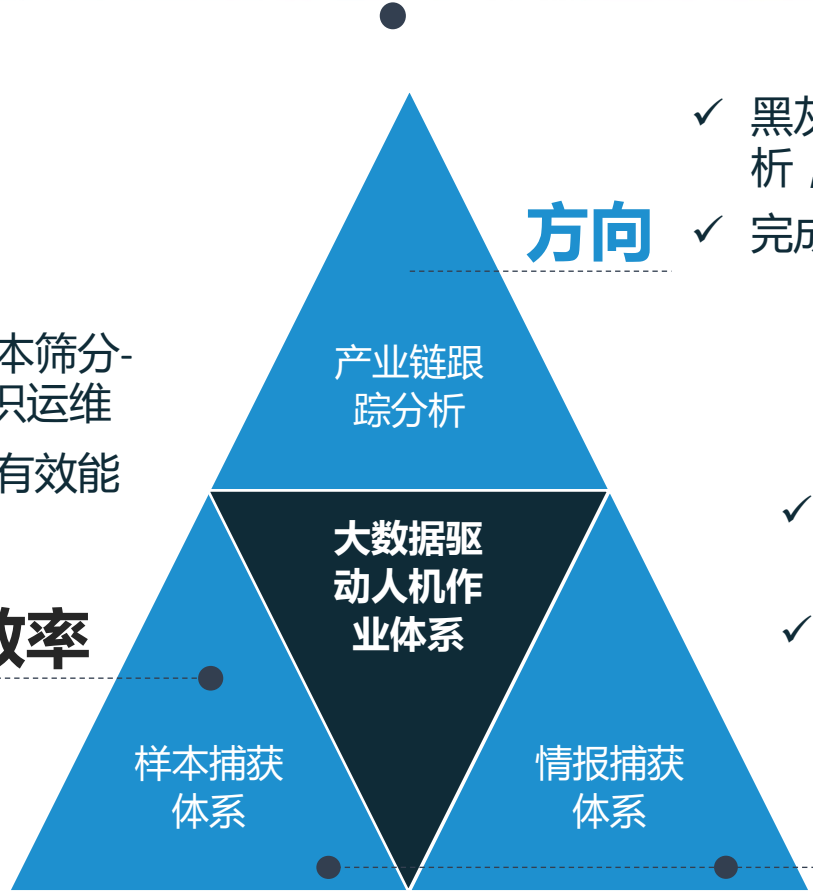
移动应用风险识别能力

移动应用反病毒引擎——精细化应用分析与标定能力





移动风险应用治理体系



方向

- ✓ 黑灰色产业链进行持续跟踪与分析，深入了解产业链游戏规则
- ✓ 完成黑灰产对抗的顶层逻辑设计

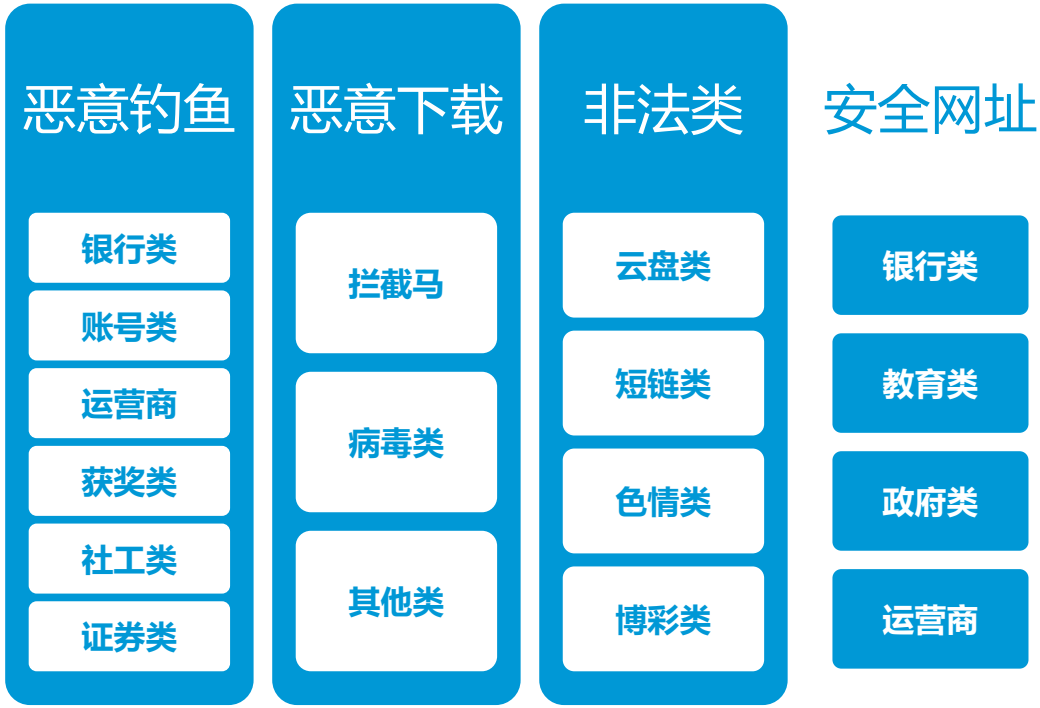
效率

- ✓ 自建全世界领先的海量样本筛分-大数据+专家智能分析-知识运维
- ✓ 海量样本高效运维和持续有效能力输出

基石

- ✓ 实现全网海量样本捕获，累计样本量十亿级，日捕获量十万级
- ✓ 掌握近万个黑灰产沟通社交群，为黑灰产情报和关键样本持续收集提供关键支撑

URL风险检测能力



全面识别恶意、非法类网址，杜绝企业终端被钓鱼的可能。

本地检测
URL规则库前置化，超强检测能力无惧网络环境变化

独有启发式能力
在保证极低误报率的前提下，为用户提供对URL样本的启发识别能力

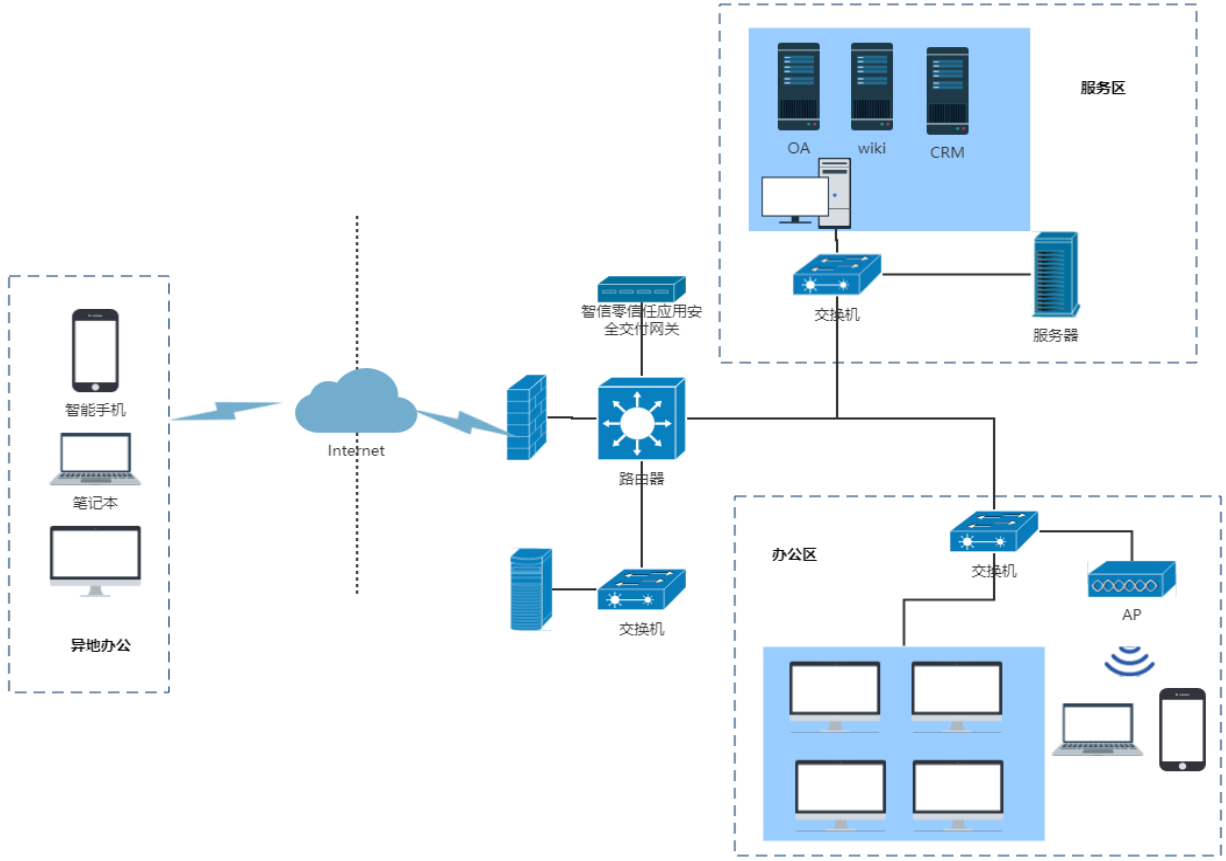
精细化标签运营
海量网址后端自动化标签运营，并结合人工分析经验，形成独有的网址精细化分析

合作伙伴针对性运营
对合作伙伴用户访问URL针对性运营强化，提高规则的有效性，提升实际防护效果

04 移动办公方案实际案例

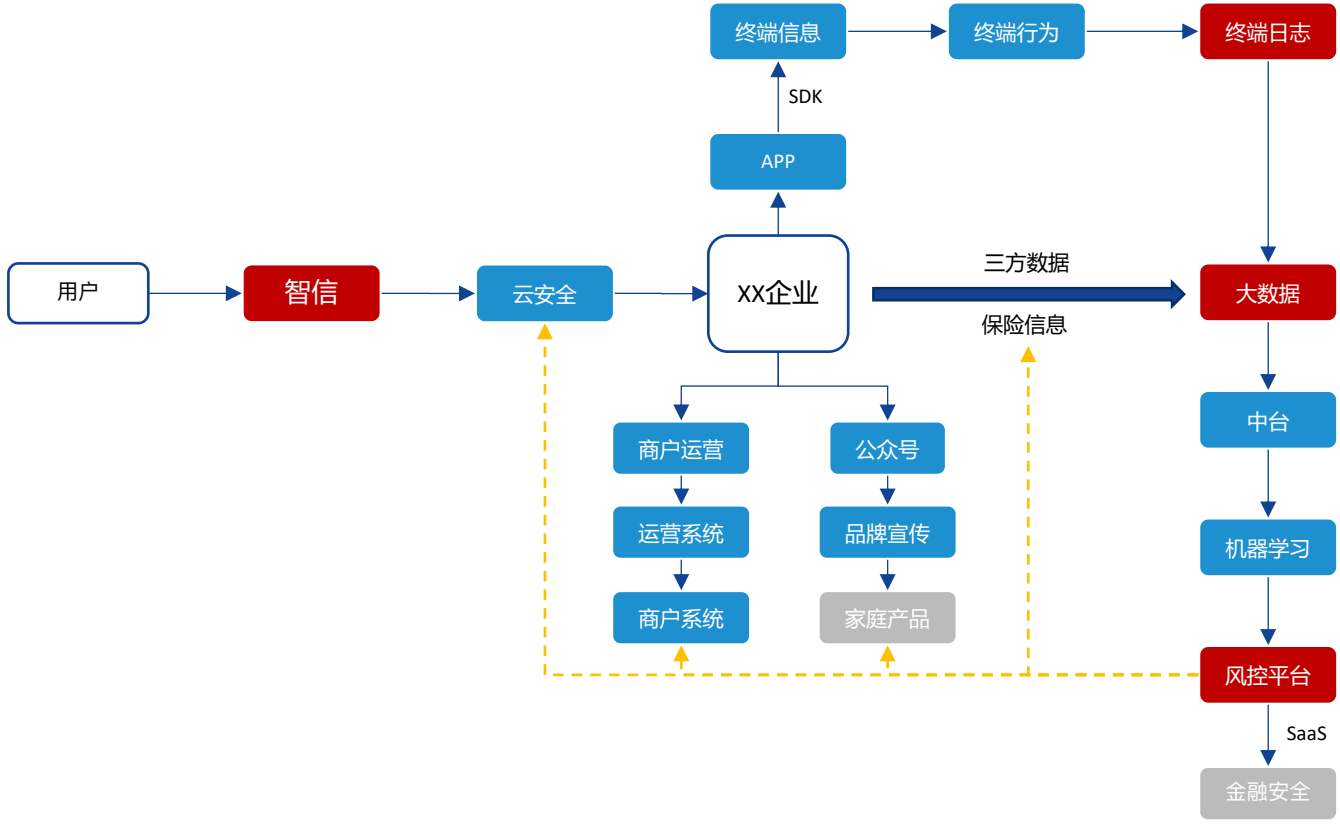
解决方案案例一

2020年，该解决方案应用于XX市某个政府单位，用于替代原协同办公平台，为移动办公数据资产全生命周期的安全保驾护航。

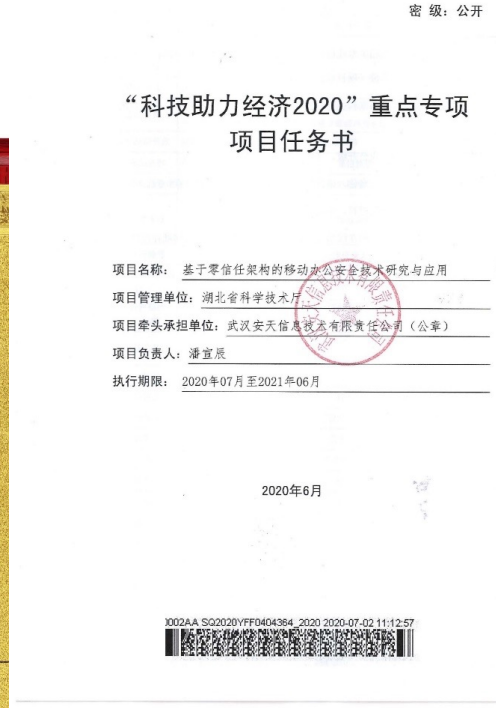


解决方案案例二

2021年，XX企业需要云服务和移动端安全地访问办公业务，安天提供的移动办公解决方案，给他们做云安全和业务数据安全保障。



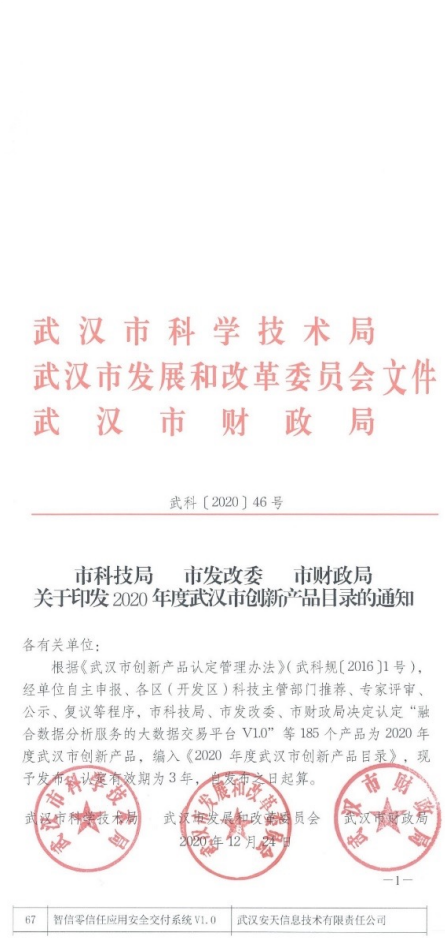
解决方案多次被评为推荐产品


密 级：公开

“科技助力经济2020”重点专项
项目任务书

项目名称：基于零信任架构的移动办公安全技术研究与应用
项目管理单位：湖北省科学技术厅
项目牵头承担单位：武汉安天信息技术有限责任公司（公章）
项目负责人：潘宜辰
执行期限：2020年07月至2021年06月

2020年6月


武 汉 市 科 学 技 术 局
武汉市发展和改革委员会文件
武 汉 市 财 政 局

武科〔2020〕46号

市科技局　市发改委　市财政局
关于印发2020年度武汉市创新产品目录的通知

各有关单位：

根据《武汉市创新产品认定管理办法》（武科规〔2016〕1号），经单位自主申报、各区（开发区）科技主管部门推荐、专家评审、公示、复议等程序，市科技局、市发改委、市财政局决定认定“融合数据分析服务的大数据交易平台V1.0”等185个产品为2020年度武汉市创新产品，编入《2020年度武汉市创新产品目录》，现予发布。认定有效期为3年，自发布之日起算。

武汉市科学技术局　武汉市发展和改革委员会　武汉市财政局
2020年12月24日

—1—

67	智信零信任应用安全交付系统V1.0	武汉安天信息技术有限责任公司

解决方案多次被评为推荐产品

湖北省经济和信息化厅办公室

省经信厅办公室关于公布第三批
免费云产品和服务目录的通知

各市、州、直管市、神农架林区经信局，各有关企业：

为帮助企业和社会各界全力做好新冠肺炎疫情防控工作，省经信厅公布了两批疫情期间可供免费使用的云产品和服务目录。该项工作开展以来，得到了省内外云服务商的大力支持和踊跃参与，经遴选、汇总，现公布第三批免费云产品和服务目录，共251项，其中疫情工作类79项，生产保障类148项，生活服务类24项。

请各地经信局认真组织本地企业按需对接，充分利用云计算、大数据等信息化手段加强疫情防控工作，为坚决打赢疫情防控阻击战贡献力量。

附件：新冠肺炎疫情期间可供免费使用的云产品和服务目录（第三批）

（联系人：曾旷怡　13607110606　邮箱：377508607@qq.c

湖北省经济和信息化厅办公室
2020年2月26日

			文档也无法打开。被授权人仅能在授权权限规定范围内查看文档。集成，嵌入或拷贝到的文档可提示是否需要授权。注册金甲DRM只插即可，界面与微软类似，使用简单方便。目前可提供PC版本下移动预计3月中旬上线。		
77	武汉安天信息技术有限责任公司	智信零信任应用安全交付系统	智信零信任应用安全交付系统主要实现线上办公的安全问题，也可完成OA系统的移动化安全迁移，有效解决目前企业网上办公移动化办公的安全性难题。该系统是在零信任安全架构基础之上，为企业建立一套完整的虚拟安全边界的应用访问环境。 1、通过统一身份认证、单点登录和链路透明加解密为企业提供应用安全访问入口； 2、通过web应用移动化和终端环境检测为企业提供低成本的安全移动办公环境； 3、通过身份、状态、行为、内容的零信任策略，为企业提供动态访问控制，以此保障应用访问安全性； 4、通过数字水印等为企业数据资产全生命周期保驾护航。	电话沟通需求	钟将伟 17762515410
78	宜昌城市云计算中心有限公司	免费云资源	城市云开放免费云资源盛情，包括云服务器、存储产品等基础云资源，让中小企业复工无忧。免费期间遵守当地政府主管部门复工复产安全管理规定。	电话沟通需求	王　曦 13469864903
	荆州九合智造		基于saas模式的为迈智造系统帮助制造业企业管理从接到订单开始到产品发货的		

武汉东湖新技术开发区　武汉东湖国家自主创新示范区　中国（湖北）自由贸易试

Wuhan East Lake High-tech Development Zone　National Innovation Demonstration Zone　China (Hubei) Pilot Free Trade Zone Wuhan

首页　走进光谷　自贸区　光谷新闻　光谷园区　创新光谷　光谷招商　光谷人才　网上服务　政务公开　ENGLISH　请输入搜索关键

当前位置：首页 > 通知公告 > 通知 > 正文

关于东湖高新区首批科技企业抗击疫情创新应用案例与技术产品清单的公

发布时间:2020-03-20　来源:　【字体：大 中 小】

各有关单位：

按照科技部火炬中心《关于开展科技企业疫情防控创新案例调研与技术产品状况汇集工作的通知》（国科火字〔2020〕59号）精神，经网上公开征集、企业自报等方式，我们梳理形成了东湖高新区首批科技企业抗击疫情创新案例与技术产品清单（见附件），为推动更多新技术新产品新服务应用于疫情防控和复工复产的准备工作，现予以公示。

该清单中的技术产品和服务涵盖病毒检测、疫情监测分析、医疗服务保障、办公生产、生活服务及其他等6个方面，有的取得了主管部门批准文号，有的有实际应用场景，有的已投入到抗击疫情和复工复产，国内外有相关需求的单位、机构、社区可直接与清单所列的各企业联系人联系洽谈。如有疑问可在3月22日之前向东湖新技术开发区产业发展和科技创新局进行反馈。

联系人：李春龙　67880552　373002626@qq.com

抗击疫情创新应用案例和技术产品清单（公示文件）.pdf

武汉东湖新技术开发区管理委员会
2020年3月20日

89	武汉安天信息技术有限责任公司	信零信任应用安全交付系统	智信零信任应用安全交付系统主要实现在疫情期间政企线上办公的安全问题，也可完成OA系统的移动化安全迁移，有效解决目前企业网上办公移动化办公的安全性难题。该系统是在零信任安全架构基础之上，为企业建立一套完整的虚拟安全边界并提供更加安全的应用访问环境。 1、通过统一身份认证、单点登录和链路透明加解密为企业提供应用安全访问入口； 2、通过web应用移动化和终端环境检测为企业提供低成本的安全移动办公环境； 3、通过身份、状态、行为、内容的零信任策略，为企业提供动态访问控制，以此保障应用访问安全性；	1、某省光电集团公司，为集团建设移动安全建设解决方案。 2、	著作权：2019SR1045583 软件产品证书：鄂RC-2019-1024-、汉RC-2019-1274-	公安部网络
90	武汉锚立信息科技有限公司	锚立设备管理系统	系统可协助企业构建设备生产数字化运营管理平台，服务于企业内部协作以及与设备供应商的远程协同支持，优化工作的安排、沟通、执行和跟进，减少不必要的面对面协调沟通，降低疫情风险；同时减少人员差旅现场作业，控制设备故障及运维成本，系统还提供员工健康管理平台，实时关注员工健康，助力企业安全复工复产。	广东		

中华人民共和国工业和信息化部

Ministry of Industry and Information Technology of the People's Republic of China

邮箱登录　移动版网站　工信微报　RSS订阅　统一搜索　看新闻　找文件　查办事　提意见　查数据　要投诉

工业和信息化部　新闻动态　政务公开　政务服务　公众参与　工信数据　专题专栏　疫情防控专题

首页 > 新闻动态 > 工信动态 > 司局动态 > 正文

工业和信息化部中小企业局关于印发《中小企业数字化赋能服务产品及活动推荐目录（第一期）》的通知

发布时间：2020-04-21　来源：中小企业局　分享：

工企业函〔2020〕87号

各省、自治区、直辖市及计划单列市、新疆生产建设兵团中小企业主管部门，有关单位：

为贯彻党中央、国务院有关复工复产和提升中小企业专业化能力决策部署，深入实施《中小企业数字化赋能专项行动方案》，征集筛选8大类、118家服务商的137项服务产品及活动，形成《中小企业数字化赋能服务产品及活动推荐目录（第一期）》，现予以印发。请结合实际，积极推动中小企业自主选择对接使用，引导“专精特新”中小企业率先通过数字化赋能成为标杆中小企业，及时总结成效，加强宣传推介，促进中小企业复工复产、加快转型。

如发现存在虚假宣传、强制使用、乱收费、失信、违法等情况的，一经查实，立即调整出《推荐目录》。

请按照《关于推动落实<中小企业数字化赋能专项行动方案>的通知》（工企业函〔2020〕69号）要求，继续支持做好每季度组织推荐工作，于季度结束15个工作日内将有关材料发送至szhfn20200163.com。

八、网络和数据安全类（4家）

序号	服务商名称	产品或活动名称	主要功能与特色	服务对象	咨询电话
1	北京科蓝软件系统股份有限公司	科蓝软件 CSIIVP eID认证合一网络身份验证平台	整合优势资源提供通用箱网络身份验证能力，打造互联网银行底层基础设施，构建最安全的互联网用户实名制身份验证平台。	银行、金融、政务	13911017066
2	武汉安天信息技术有限责任公司	智信零信任应用安全交付系统	为企业建立完整的虚拟安全边界并提供安全可靠的应用访问环境，助力企业低成本构建安全移动办公环境。	有安全需求的各行业中小企业	027-87668767 17762515410
3	价值链技术（深圳）有限公司	区块港机器人	支撑技术、业务、数据融合、实现层级、地域、系统、部门、业务整合。解决信息孤岛、数据主权在安全信任基础上，实现多方融合、高效协作。	工业及园区、创业综合体、高校、分布式能源提供商等	13811790624

感谢大家的关注

安天冬训营 wtc.antiy.cn