

指掌易金融行业移动安全 解决方案



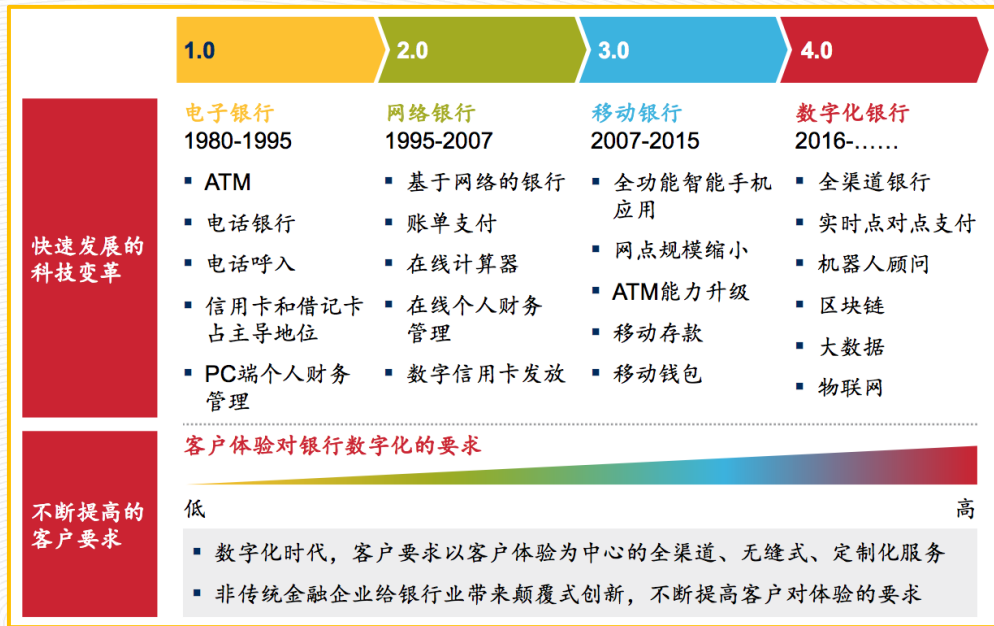
指掌易科技

**金融行业正在快速数字化转型，
移动信息化成为业务与技术的联结纽带**

金融行业尤其是银行业全面步入数字化时代

银行业“转型+创新”的双轨战略： 以客户为中心 + 全面数字化

麦肯锡研究了30多家全球领先银行的发展案例，结合中国市场趋势和行业发展现状，发现全球领先银行不约而同采取了“转型+创新”的“双轨战略”。**一方面推动传统业务向以客户为中心的商业模式全面转型；另一方面以数据及科技为引领，全面布局数字化。**



引自：<http://www.mckinsey.com.cn/中国银行业的明天在哪里-双轨战略/>

全球领先银行正大力推进数字化改造



引自: <http://www.mckinsey.com.cn/中国银行业的明天在哪里-双轨战略/>

客户体验成为领先银行的成功之道

截至2016年，中国互联网金融市场对网民的渗透率已达70%，用户数突破5亿人

理财

- 互联网理财分流存款严峻，2016年互联网理财规模达到

26,000亿元
人民币



8,083亿元¹

贷款

- P2P网络贷款的交易规模已超过

20,600亿元
人民币



8,000亿元²



60,000亿元³

支付

- 第三方互联网+移动支付交易规模已超过

105万亿元
人民币



408,400亿元⁴



255,000亿元⁴

¹ 2016年底理财规模

² 截止2016年底，累计放贷总额

³ 截止2016年底，累计交易量

⁴ 2016年交易额

中国互联网信息中心 (CNNIC); 艾瑞咨询 (iResearch); 麦肯锡分析

麦肯锡调查显示：中国领军金融企业已对国内传统银行业务产生了颠覆式的影响

- 驱动要素之一：传统增长手段难以维系增长
- 驱动因素之二：金融科技企业倒逼银行业提升客户体验
- 驱动因素之三：客户行为变革后，提升客户体验成为必须
- 驱动因素之四：颠覆式技术——提升客户体验的重大机遇

引自：<http://www.mckinsey.com.cn/客户体验：领先银行的成功之道/>

移动优先是众多金融企业改善客户体验的首要选择

在新一代银行架构中，要以客户为中心，就要落实全渠道建设思维，最重要的一点就是“移动优先”。

移动互联本身就是将业务以数字化方式交付，既是业务概念，又是技术概念，是联结金融业务与金融科技的纽带。



对外，领先银行已经提供诸多移动金融自服务应用

银行	公共移动App数目*
工商银行	23
建设银行	9
农业银行	9
中国银行	42
交通银行	7

银行	公共移动App数目*
兴业银行	7
招商银行	8
民生银行	10
浦发银行	6
中信银行	7
光大银行	8
平安集团	47
华夏银行	6

银行	公共移动App数目*
北京银行	5
上海银行	4
江苏银行	3
南京银行	3
宁波银行	5
杭州银行	6
贵阳银行	2
常熟银行	3
无锡银行	2
江阴银行	1
张家港银行	4
吴江银行	2

几乎所有领先银行都在面向用户直接提供移动应用，包括支付、融资、理财、交易等主要金融服务。

资产规模前25位银行，发布在iOS App Store中的移动App数目合计就达到229个。除去平安集团外，最多的中国银行就有42个App发布。

*数据统计自iOS App Store中各家银行发布的App，2017.9.13

*平安银行包含在平安集团中

*银行资产规模数据来自Wind资讯

对内，为优化业务及协作效率也提供诸多业务线和移动办公应用



LOB业务线

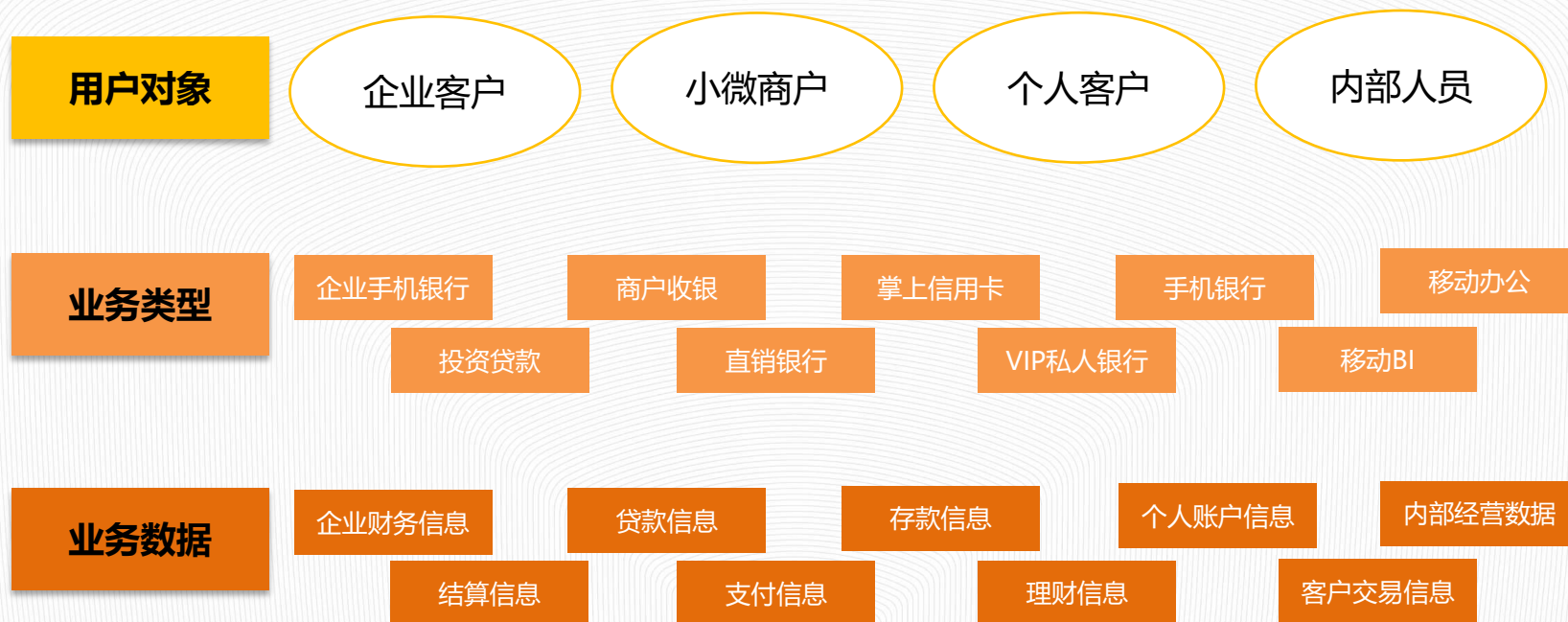
- LOB业务移动化，主要是统一配发专用移动智能设备，在平板、手机上实现移动营销、移动信贷、财富管理、移动开卡、移动VTM等业务。
- 相较于对外提供的移动应用，借助于有人面对面的服务，能够提供个性化金融服务，实现更佳的用户体验。



移动办公

- 移动办公，主要形式为BYOD员工自带设备，解决协同办公审批、手机邮件、文档协作、移动BI、人事行政服务、系统监控预警等内部需求。
- 移动办公大幅提升了企业内部的协作效率，增强了内部信息透明度，从而提高企业的竞争力。对于银行、证券、保险、投资等传统金融企业，也是面对互联网金融等新金融形态挑战的必由之路。

业务移动化的广泛使用也带来了敏感业务流程和数据泄露的更多风险



对外，当前的威胁本质上是来自于广泛的使用者可能对应用漏洞的利用



- 对外的移动应用发布后，任何人都可以轻松获取到，包括各类恶意用户。
- 恶意用户本身也可以成为真实的目标用户，无法从用户身份上屏蔽。
- 对漏洞的利用，需要一定的专业技能，普通用户难以具备此类技能。

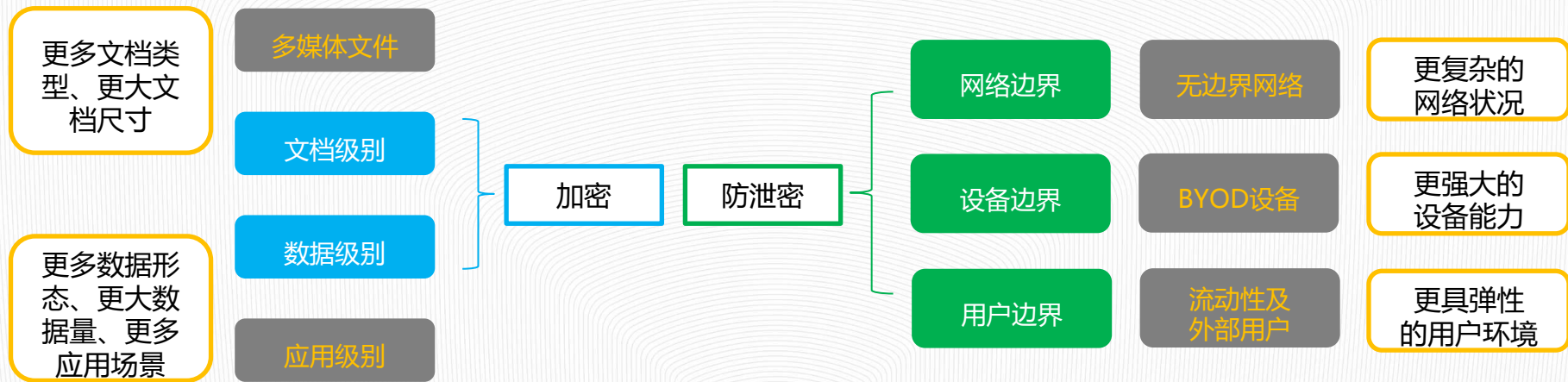
新民晚报 新民网
xinmin.cn

黑客利用理财APP漏洞半天提现千万 上海破获特大网络盗窃系列案

新民晚报 09-15 12:42

对内，当前最主要的威胁则来自于内部敏感数据的外泄

敏感数据外泄的风险，在PC端同样会存在，但是在移动时代，更加便捷、智能、互联网在线的移动设备，既有利于业务和办公，同时也会带来更大的数据防泄露挑战。



研究机构也指出：用户盗取数据对企业造成的威胁远比恶意软件要严重得多

- CISO 不确定仅依靠 EMM 就能满足移动安全的全部需求，还是应该再结合使用一些其他的移动安全工具
- 随着移动安全工具数量不断增加，CISO需采取正确的方法将其与 EMM 解决方案进行整合
- 目前对很多企业而言，**用户盗取数据对其造成的威胁远比恶意软件要严重得多**

Gartner: When and How to Go Beyond EMM to Ensure Secure Enterprise Mobility, 19 Jan 2017

金融业移动安全的实践之路

技术安全

业务安全

过去几年：第一阶段

传统IT思维、面向短期安全问题

- 以代码安全为出发点，对向外发布的应用使用App加固技术重点防护
- 以管理为中心，在内部使用 EMM平台管理配发设备

现在进行时：第二阶段

移动化思维、保护核心数据安全

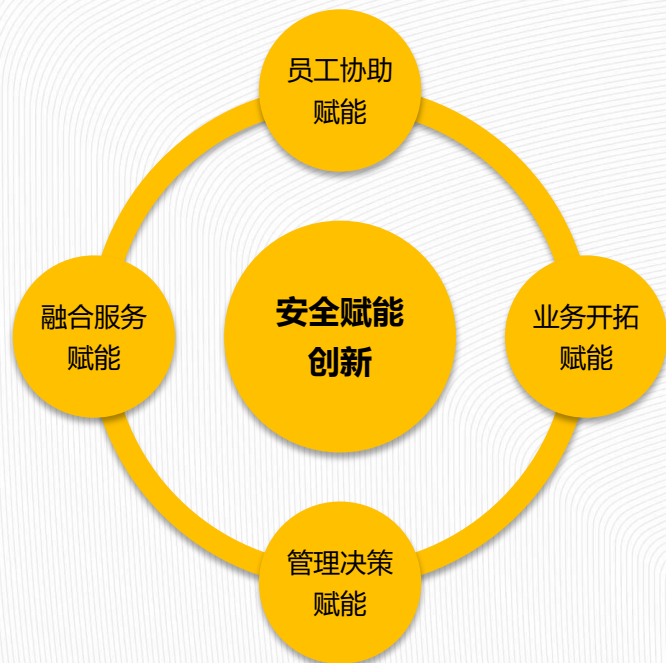
- 面向数据安全，构建场景化的应用级移动安全平台
- 以服务为中心，面向BYOD时代强调用户体验
- 平台轻量化，快速迭代演进

即将到来：第三阶段

数字化思维、无缝融合安全与业务

- 面向移动优先战略，构建整合的移动安全平台，一站式解决各种移动安全问题
- 在解决了简化IT安全管理与用户体验问题的基础之上，以创新为中心，推进企业数字化竞争能力

金融业多种业务场景安全赋能需求



为员工协作赋能

- BYOD移动办公
- 手机邮件
- 知识文档协作

为业务开拓赋能

- 移动智能POS
- 智能银行：VTM、厅堂理财
- 移动银行：移动信贷、移动营销
- 数据采集：移动双录/ATM设备巡检/网点样板采样

为管理决策赋能

- 移动BI（领导管理驾驶舱）
- 无纸化会议

为融合服务赋能

- 移动应用加固
- 移动应用风险检测

金融业移动安全需要解决一系列问题

- 成千上万的移动终端如何才能高效纳入统一管控？如何实现有效的资产管理、设备定位追踪、及时掌握设备使用状态？
- 如何有效按需管控设备功能、设置合规策略并以有效手段处理违规事件，从而有效规范设备的使用行为？
- 如何有效应对统配终端和BYOD自带终端混杂的复杂局面？如何在一部终端上有效隔离公私应用和数据？
- 业务应用从何处获取？业务应用更新如何及时下发安装？业务应用越来越多应该如何有效统一管理？应该如何限制使用者私自安装非工作相关应用，如何及时跟踪应用使用行为？
- 移动设备承载大量业务信息、用户信息等敏感数据，应该如何有效保护这些数字资产的本地存储安全和传输安全？应该如何有效防护这些数字资产不被有意或无意泄露出去？
- 在接触客户的业务环节中社交类移动应用被广泛使用，应该如何及时掌握这类应用的使用行为和信息内容，及时发现其中的违规违法行为以避免对客户和企业造成损害？
- 上述问题的解决方案是否具有对移动终端设备、移动应用、现有IT设施的良好兼容性？是否具有赋能业务移动化推进的能力？

设备

应用

数据

行为

满足金融行业相关信息安全合规要求

指掌易金融业移动安全与管理解决方案

指掌易提供完整的移动安全与管理能力



□ 全平台: H5、iOS、Android
 □ 全要素: 设备、应用、数据、文档、身份、网络
 □ 全功能: 云-管-端的整体移动安全
 □ 全局视角: 从单点应用、单点设备到全局

指掌易方案主要功能模块能力分解

移动设备管理

用来管理设备资产、远程配置、安全策略、功能限制、合规策略、远程控制、定位追踪等；

移动应用管理

提供企业应用商店、应用推送、应用黑白名单、应用安全策略等；

移动安全工作空间

基于VSA技术提供的应用级虚拟安全域环境，隔离个人与企业业务数据，并为企业搭建专属应用商店，提供业务移动化统一门户入口；

数据防泄露DLP

提供完整且灵活的数据防泄露管控策略，具备数据加密、动态水印、禁止复制/粘贴、禁止截屏/录屏、禁止系统功能调用、禁止多媒体访问等能力，并可按需细粒度化调整管控策略；

安全接入隧道

为安全业务应用建立应用级安全传输通道，保护数据传输安全，可针对应用和用户执行双重准入控制和过滤，并可广泛兼容第三方VPN集成；

安全办公组件

提供开箱即用的安全邮件、安全IM、远程协助、安全浏览器和安全云盘办公组件，组件原生预置完整DLP安全属性，可与现有移动办公方案轻松整合；

移动内容审计

支持手机通话记录和短彩信记录的审计，支持对常用社交类工具的聊天文字、图片、语音、视频、语音通话等内容实施审计，并可对常用社交类工具的红包及转账进行审计等；

开放扩展能力

可无缝整合第三方移动安全服务能力，如移动应用病毒查杀、漏洞扫描、安全加固等。

为各种金融业务移动化场景提供安全和管理保障

业务场景		中后台转型			前台转型			用户
	管理层	IT运维	投资研究	业务内勤	客户经理	服务经理	厅堂经理	金融用户
1.BYOD移动办公	★		★		★	★	★	
2.手机邮件	★	★	★		★	★	★	
3.移动知识管理	★	★	★		★	★	★	
4.智能银行							★	★
5.移动银行-客服					★			★
6.移动银行-收单 (含智能POS机)								★
7.移动银行-信贷					★			
8.移动银行-财富管理					★			
9.移动BI(管理驾驶舱)	★							
10.保险移动展业					★			
11.保险移动理赔						★		
12.公众自服务App								★

中后台业务移动化场景

金融业BYOD移动办公： EMM方案已经越来越不适用于BYOD场景

不合适的EMM方案

用户体验

需要繁琐的设备注册过程
收集过多的用户隐私信息
智能设备能力受到太多限制

IT运维

管理范围过大
管理过程太过复杂
知识与技能要求过高

技术实现

依赖于MDM
实施过于复杂
迭代周期太长

合适的BYOD安全方案



金融业BYOD移动办公：指掌易BYOD移动安全工作空间解决方案

业务场景

- 用户为内部各类人员，使用自带BYOD设备移动办公
- 移动办公可能包括：收发企业邮件、访问企业内网系统、进行办公审批、查看内部文档等

安全挑战

- 邮件、OA、审批等多个移动办公应用，需要安全分发应用到每个用户手机上，并且能及时进行版本更新
- 办公应用产生的文档等数据，如邮件附件、OA文档等，在设备上未进行加密，易于被其他应用获取外泄
- 使用手机邮件、访问内部网站时，可以使用复制/粘贴将企业内部信息泄露给外部人员
- 在使用办公应用时，用户很容易就可以进行应用截屏，将办公信息以图片方式外泄
- 合法用户进行移动办公时，手机屏幕可能被拍照后泄露企业信息，并且无法追溯拍照源头
- 现有MDM/EMM方案需要用户注册手机，严重影响用户体验，且IT管理复杂度过高，难以真正推广
- 合法用户需要便捷地接入内网办公系统

指掌易方案

□ 方案简介

指掌易BYOD移动安全工作空间解决方案，无需MDM设备管控，直接面向业务安全，向企业交付私有的移动应用商店的同时，实现通用的、轻量级、自动化移动数据防泄露能力。
可配套提供移动安全邮件、安全IM、安全浏览器以及安全云盘，解决企业移动办公最常用的通用协作需求。

□ 关键字

BYOD、用户体验、数据防泄露DLP、动态水印、应用级安全接入隧道

□ 主要功能

- 企业应用商店：个性化、应用多版本支持
- 基于应用级策略的DLP：应用数据加密、防止复制/粘贴、防止截屏等
- 应用界面动态水印：绑定用户名
- 应用级安全接入隧道，为移动应用连接内网提供安全通道
- 开放扩展能力：支持与现有移动OA等门户深度整合

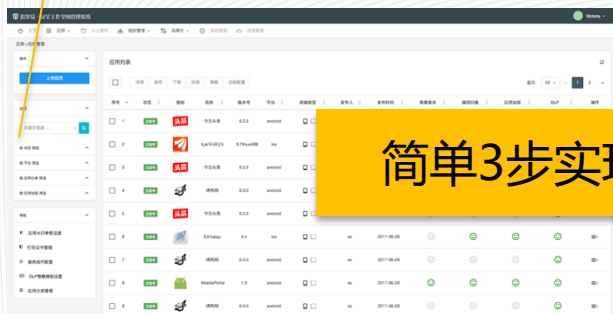
□ 业务价值

- 无需MDM，优秀的用户体验，简化BYOD移动办公推广过程
- 业界顶级自动化、即时应用封装技术，实施快速简便
- 开放可扩展、轻量级平台，一站式解决移动安全问题

金融业BYOD移动办公：指掌易移动安全工作空间解决方案

- 无需管理设备，直接保护应用
- 无需开发商介入，自动化封装保护
- 保护策略动态化、个性化、实时化

- 个性化的企业私有应用商店，方便用户安全、便捷开展移动办公
- 只限工作应用提供的内网访问能力



1. 管理员后台发布应用，同时指定应用DLP策略

简单3步实现安全保护！



2. 用户下载安装安全工作空间客户端



3. 用户从安全工作空间中安装并开始使用工作应用

- 没有繁琐的设备注册过程
- 不需要获取高级设备权限
- 不收集用户个人隐私信息

金融业手机邮件：指掌易移动安全邮件解决方案

业务场景

- 移动办公的典型场景就是手机收发邮件
- 用户主要使用BYOD个人手机
- 除了邮件外，还需要同步日程、企业通讯录等

安全挑战

- 邮件信息在移动设备上未加密，并且很容易泄露出去
- 邮件正文可能被截屏、复制/粘贴到外部，并且无法追踪到泄露源头
- 邮件附件在访问时，可能被从本地分享到外部
- 任意移动设备均可接入收发邮件，缺乏设备准入管控
- 用户可能从不同的应用商店下载不同的邮件客户端，其中可能包括被重新打包的高风险客户端
- IT部门对手机邮件的相关问题提供支持时，需要面对不同的邮件客户端，邮件配置方法各不相同，大大提高了支持复杂度
- 邮件传输可能在非安全网络下进行，邮件信息在传输过程中容易被第三方截取

指掌易方案

□ 方案简介

指掌易移动安全邮件解决方案，面向BYOD环境，为Android、iOS提供标准的企业级邮件客户端，支持多种邮件协议和配置，结合安全工作空间平台，为用户提供优秀统一的邮件体验，为IT部门提供完整的邮件数据安全保护。

□ 关键字

跨平台统一邮件客户端、数据防泄露DLP、动态水印、自动配置

□ 主要功能

- 支持多种设备及平台，支持多种邮件及文档客户端
- 多种邮件协议支持：Exchange ActiveSync、IMAP、POP
- 邮件DLP保护：附件数据加密、防止复制/粘贴、防止截屏、动态水印
- 集中远程邮件客户端自动化配置
- 新邮件实时推送通知

□ 业务价值

- 端到端的统一企业级移动邮件安全管理
- 完整的邮件数据防泄露能力
- 简化办公邮件使用，推进BYOD移动化战略

金融业手机邮件：指掌易移动安全邮件解决方案



- 面向iOS、Android一致的用户体验
- 优雅简洁的邮件客户端界面
- 新邮件实时推送通知
- 丰富的邮件、文件夹同步能力
- 邮件数据加密、防止复制粘贴、水印/防截屏等安全保护

- 复杂参数配置交给后台集中配置：邮件服务器地址、协议、端口、配置
- 个性化设置用户自己决定：字体、签名、列表风格
- 快速的系统适配：iOS 11 当日适配



金融业移动知识管理：指掌易移动文档安全协作解决方案

业务场景

- 在办公、投资、管理等金融企业的各种工作过程中，越来越多需要从手机上随时随地访问工作文档
- 更需要安全地与他人充分进行文档协作以利用知识

安全挑战

- 工作文档很多时候包含敏感信息，不能随意带出企业网络环境，例如客户信息文档、合同文档、资产评估报告、“双录”音视频资料等等
- 不同业务人员具有不同的权限，在移动端需要限制其访问的工作文档范围
- 企业内部文档在移动端使用时，未加密的文档会在移动设备上暂存，存在泄露风险
- 快速的业务开展过程中，用户经常采用微信、QQ等互联网工具发送企业文档
- 文档在移动端打开时，存在通过复制/粘贴、截屏等方式将重要信息外泄的高风险
- 一旦整个文档或部分内容外泄后，难以追溯到源头

指掌易方案

□ 方案简介

指掌易移动文档安全协作解决方案，提供Android、iOS跨平台支持，为企业提供统一的移动安全文档服务平台，支持工作文档的选择性分发、文档DLP安全保护、文档协作安全保护。

□ 关键字

文档数据防泄露DLP、动态水印、跨平台、文档协作安全

□ 主要功能

- 私有云盘，支持多种设备及平台
- 工作文档可控分发
- 文档DLP保护：文档数据加密、防止复制/粘贴、防止截屏、动态水印
- 文档外链安全保护：有效期、下载次数
- 文档采集、回传、同步
- 组织架构集成，统一的文档分发和管理服务平台

□ 业务价值

- 完整的文档数据防泄露能力
- 轻量级、面向移动端的安全文档协作平台
- 多种使用模式支持：企业知识库、私有云盘、分享协作
- 简化的基础架构，无需复杂的专业存储技术人员

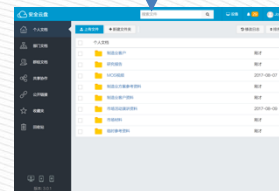
金融业知识文档协作：指掌易移动文档安全协作解决方案

使用场景一：企业知识库模式
管理员上传企业知识文档，分配到部门、群组或用户并指定权限



使用场景三：分享协作模式
用户A分享文档给用户B，并指定安全策略，用户B可以安全访问使用

使用场景二：私有云盘模式
用户A上传个人文档，在PC、移动端，在内网、外网都能随时同步并安全访问使用



外网

DMZ区

内网

金融业移动BI（管理驾驶舱）：指掌易移动BI数据防泄露解决方案

业务场景

- 金融行业竞争越来越激烈，从管理层到业务层，都需要能快速获取业务数据，并借助可视化分析，迅速进行决策以应对瞬息万变的市场需求，移动BI价值凸显

安全挑战

- BI涉及的数据，尤其是分析结果数据，是汇总了各类业务的综合数据，是用于辅助决策的业务信息，其价值比一般个体数据更大。
- 移动BI需要在移动设备上访问这些关键的业务决策支持信息，相关信息的防泄露格外重要
- 移动端天然的便利性，导致分享、截屏、拍照等十分便利，导致相关的BI数据、图表等很容易外泄
- 越来越多的用户，包括管理层领导，在访问移动BI系统时，偏好于使用个人自带的BYOD设备，包括个人手机、平板等，使得企业对于移动BI应用所运行的环境无法进行控制，提高了保护业务数据的难度

指掌易方案

□ 方案简介

指掌易移动BI数据防泄露解决方案，基于指掌易领先的移动DLP技术，在不影响移动BI用户使用体验的前提下，无需设备级管控，直接对BI应用进行防泄露保护。

□ 关键字

移动DLP、安全接入、远程擦除

□ 主要功能

- 移动DLP（数据加密、防复制/粘贴、防截屏、动态水印）
- 应用级按需移动安全接入
- 远程应用锁定及数据擦除
- 开放扩展能力，客户端生物识别认证

□ 业务价值

- 保护核心高价值BI数据
- 业界最高效的移动DLP保护，确保业务数据安全
- 移动DLP实现过程，无需BI应用开发商配合
- 优秀的用户体验，对用户无影响

金融业移动BI（管理驾驶舱）：指掌易移动BI数据防泄露解决方案

移动BI全生命周期移动数据防泄露保护



安全分发应用，控制设备准入



数据传输与落地加密



远程禁用与擦除数据



动态水印绑定到人，责任溯源

前台业务移动化场景

智能银行：指掌易智能银行移动安全管理解决方案

业务场景

- 越来越多银行，通过VTM等智能设备提供7×24小时智能金融服务，扩展服务时间和能力，节省运营成本
- 使用多种形态的智能设备，包括移动智能设备

安全挑战

- 设备资产分散，电源、内存、网络等各种可用状态不能随时掌握，设备的可用性不可控，最终影响业务的正常进行
- 向各种分散的智能设备上，分发、安装、更新、卸载智能应用过程复杂，且带来过多的信息交互，进而导致安全隐患
- 使用的通用智能设备如平板电脑等，存在太多在智能银行网点中不需要的功能和信息传输能力，如蓝牙、GPS、USB等，带来额外的安全隐患
- 冗余的功能和能力，也会分散使用者的注意力，影响正常业务效率
- 智能银行设备需要限制在特定的银行网络，人工进行网络配置既复杂又不安全
- 业务文档、宣传资料需要在设备上随时使用并更新

指掌易方案

□ 方案简介

指掌易智能银行移动安全管理解决方案，提供Android、iOS跨平台支持，基于指掌易成熟的EMM平台，无线采集智能银行环境中的各类智能设备状态、限制设备功能、管理移动应用、统一配置管理设备网络、安全分发业务文档资料。

□ 关键字

MDM、MAM、MCM、资产管理、合规管理

□ 主要功能

- 设备资产管理
- 设备功能限制与锁定、远程配置、远程擦除
- 移动应用管理
- 移动内容管理
- 自动合规处理

□ 业务价值

- 强管控场景下充分的移动安全管理能力
- 对设备、应用、内容的全生命周期管理能力，支持业务变化快速响应
- 自动化的异常通知和远程处理，简化IT运维工作

智能银行：指掌易智能银行移动安全管理解决方案



固定式智能平板



大堂经理手持平板



其他智能设备



网点内部网络

企业移动安全管理平台

- 集中管理设备状态
- 分发推送应用、内容
- 网络自动配置及准入
- 动态安全与合规策略



移动银行：指掌易移动银行移动安全管理解决方案

业务场景

- 基于移动设备+上门服务办理银行业务
- 使用移动APP办理业务
- 统一客服、移动收单、移动信贷、移动财富管理等

安全挑战

- 所有在智能银行面临的问题都会同样存在
- 更进一步，相比网点设备，展业场景更复杂，智能移动设备所在的环境位置更加分散，网络环境更加复杂
- 业务场景更加碎片化、更加复杂：
 - ✓ 由银行客户经理、财富经理等主导使用，比如移动信贷、移动财富管理
 - ✓ 由商户主导使用，如移动收单中的智能POS机
 - ✓ 由银行员工与客户共同使用，如同客VTM等
- 使用环境位置不可控，客户敏感信息容易外泄
- 在与客户交往过程中的言语行为是否合规、交流内容是否合规很难被追踪
- 可能在银行之外的网络中使用

指掌易方案

□ 方案简介

指掌易移动银行移动安全管理解决方案，综合指掌易EMM能力、移动DLP、移动安全接入、移动内容审计与态势感知能力，集中管理移动银行多种业务场景下敏感数据安全不外泄、应用级安全隧道接入银行内网、行为及内容审计以及设备状态信息统计与呈现

□ 关键字

EMM、DLP、移动安全接入、内容审计、态势感知

□ 主要功能

- EMM (MDM/MAM/MCM/合规管理/策略管理/地理围栏)
- 移动DLP (数据加密、防复制/粘贴、防截屏、动态水印)
- 应用级按需移动安全接入
- 移动内容审计 (通讯内容审计、社交类应用内容审计)
- 态势感知 (POS机位置、设备状态、故障情况等)

□ 业务价值

- 快速方便的业务应用升级推送机制，快速应对业务变化
- 业界最高效的移动DLP保护，确保业务数据安全
- 专用的应用级移动安全接入隧道，快捷、安全地接入后台业务服务
- 基础业务移动化状态信息收集，轻松掌控业务移动化

移动银行：指掌易移动银行移动安全管理解决方案

业务移动化状态掌控

敏感数据DLP保护

移动安全接入

终端安全与应用分发

统一客服



移动收单



移动信贷



财富管理



保险业移动展业与移动理赔：指掌易保险业移动安全管理解决方案

业务场景

- 移动互联网时代保险业竞争加剧，通过移动化手段可以在第一时间将客户信息、保单、申请书等资料数字化并加快业务流程。典型场景是移动展业与移动理赔。

安全挑战

- 类似移动银行场景，用于工作的移动设备分散在不同地点、不同网络，其状态需要能够实时掌握，确保业务连续性
- 用于展业和理赔的专用设备需要限制各种功能和外设，确保专机专用，并能够从外网随时安全接入
- 在展业和理赔等工作过程中，需要在移动设备上拍摄身份证、驾驶证、行驶证、护照、港澳通行证、军官证、户口本等多种证件，以及银行卡、车辆等照片，这些都会保存在移动设备本地，可能被泄露
- 还有很多信息在移动设备中会进行录入，通过截屏或拍照也很容易被泄露并难以追责

指掌易方案

□ 方案简介

指掌易保险业移动安全管理解决方案，综合指掌易EMM能力、移动DLP、安全云盘以及移动安全接入能力，在保障移动安全的同时，进一步简化业务数字化。

□ 关键字

EMM、DLP、移动安全接入、安全云盘

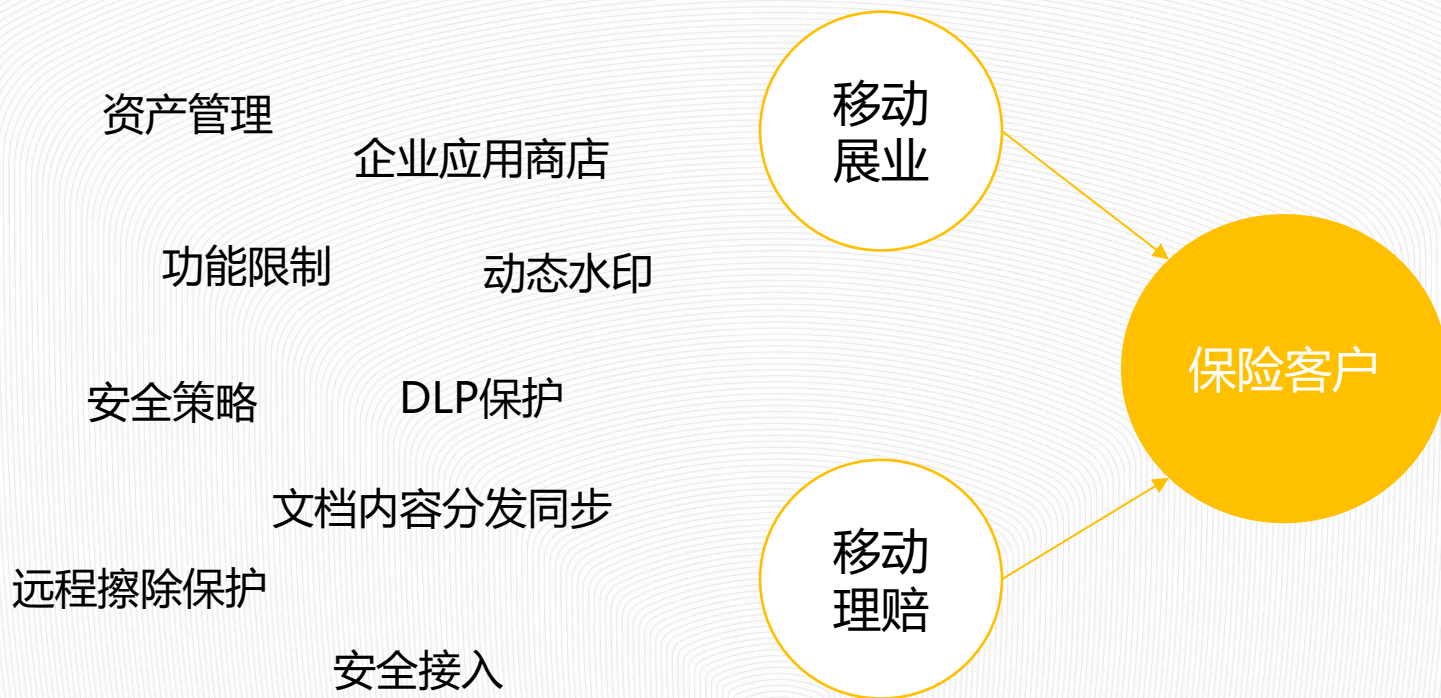
□ 主要功能

- EMM (MDM/MAM/MCM/合规管理)
- 移动DLP (数据加密、防复制/粘贴、防截屏、动态水印)
- 应用级按需移动安全接入
- 安全文档同步

□ 业务价值

- 完整的移动安全管理能力，实现端到端的安全与管理
- 快速方便的业务应用升级推送机制，快速应对业务变化
- 业界最高效的移动DLP保护，确保业务数据安全
- 专用的应用级移动安全接入隧道，快捷、安全地接入后台业务服务
- 各类业务照片和文档资料，可以通过安全云盘双向同步
- 基础业务移动化状态信息收集，轻松掌控业务移动化

保险业移动展业与移动理赔：指掌易保险业移动安全管理解决方案



公众用户自服务App场景



指掌易科技

面向公众的自服务移动App应用面临来自黑产的严重安全威胁



解决之道：指掌易移动应用安全检测与加固解决方案



安全检测

四大组件风险 脱壳解密 业务流程漏洞 HTTP传输数据风险
代码漏洞 敏感数据威胁



安全加固

界面劫持 二次打包 页面劫持（钓鱼） 模拟器运行
进程附加&注入 逆向反编译 游戏外挂



威胁监测

截屏录屏威胁 Java函数挂钩 进程注入 网络切换 代理抓包 调试器附加 软件抓包
危险软件过滤（清场） 屏幕截屏 区域变更 设备信息修改 原生函数挂钩 提权 电量过低
运营商变更 键盘输入漏洞 调试威胁 攻击框架 位置造假 盗版山寨应用



数据统计

安全大数据统计 实施邮件预警

指掌易解决方案的优势及价值

选择指掌易解决方案的理由

01 技术领先

指掌易解决方案核心技术行业领先，提供覆盖端、管、云关键节点全面的移动安全防护能力，可深入各类垂直业务场景策略化应对来自于终端、应用、数据、用户侧的各类移动安全风险。

02 生态友好

指掌易解决方案是一套生态友好型的解决方案，对各类移动终端和应用软件的碎片化高度兼容，并具有标准化集成扩展能力，可轻松融合现有IT基础设施和技术产品，可高效联合上下游伙伴为金融行业客户提供满足合规要求的一站式完整解决方案。

03 平台属性

指掌易解决方案可成为金融行业客户IT移动化建设的重要基础组件，为搭建标准、统一的业务移动化平台赋能。

04 应用实践

指掌易解决方案拥有大规模实际部署的客户成功案例，技术架构经过了移动安全实践的真实考验，指掌易科技已经成为金融行业客户值得信赖的业务伙伴

指掌易解决方案的客户价值



之于终端用户

指掌易方案可从业务应用和数据角度提供移动安全保护，有效屏蔽移动操作系统和终端型号碎片化，对BYOD环境极度友好，对于终端用户可充分保证其终端设备的使用喜好和体验。



之于IT管理者

指掌易方案对传统IT系统友好兼容，并可作为关键组件扩展移动IT功能，一体化方案功能完备、界面友好、部署灵活快速，可极大降低部署运维成本、缩短学习曲线。



之于业务管理者

指掌易方案解决了移动安全风险的专业问题，业务管理者可专心致力于领导业务运营和大众服务，并可通过方案提供的具有洞见的信息和数据进行业务决策和创新，驱动业绩目标的达成。



之于金融客户企业

指掌易方案为移动金融业务安全运营保驾护航，保护了企业的金融数字资产，也保护了用户的个人隐私信息，在满足合规要求的基础上帮助金融客户企业增强创新拓客的能力，提升品牌及市场竞争力。

指掌易解决方案的成功案例

众邦银行 – 移动展业



众邦银行
Z-BANK



客户背景介绍

武汉众邦银行成立于2017年5月，定位于专注服务中小微企业的交易服务银行，也是一家采用线上线下交互模式运营的民营银行。由于是新成立银行，正在大力进行信息化及业务系统建设，该项目隶属于武汉众邦银行对公开户系统下的移动设备管理子项目，银行为业务人员统配平板电脑利用移动展业应用上门为企业办理开户业务。



客户需求痛点

- 资产管理：由于平板配给业务人员外出使用，所以需要移动设备进行资产管理，人员信息统计；
- 数据保护：保护移动展业应用在办理开户过程中拍摄的身份证照片及录像；
- 远程控制：需要对设备远程实时定位及历史轨迹查看，对于意外情况需要远程锁定设备或者擦除数据等。



指掌易方案价值与优势

- 行业领先的移动安全核心技术
- 完整的解决方案能力全面覆盖各类安全需求
- 移动设备管理+DLP形成对单一移动设备管理方案厂商的差异化竞争优势



指掌易解决方案

- 企业移动化管理平台提供对用户设备的资产管理及人员信息统计、远程实时定位及历史轨迹查看、远程设备锁定、远程数据擦除等功能；
- 设备功能限制：移动设备管理模块限制设备蓝牙、USB传输、外置TF储存卡、修改系统时间和日期等，在设备层面杜绝一切外发方式以达到对数据的保护；
- 数据防泄露DLP：对移动展业App提供DLP保护，包括防止截屏、防止复制粘贴、应用及界面水印、应用数据加密等，其中水印可根据姓名动态生成。

凡普金科 – 移动营销



客户背景介绍

凡普金科是一家大型金融科技集团，为有借款咨询、车辆融资租赁、消费分期、理财社交、投资等需求的人提供互联网金融信息服务。公司以COPE的方式为业务员统一配发移动办公手机来提高业务效率，但同时需要有效的手段来管理办公手机的合规使用和移动信息安全，目前，业务员对于办公手机的使用行为、IM类通信内容审计以及业务数据安全等是公司重点急需解决的问题。



客户需求痛点

- 贷后业务人员通过企业版微信、微信、QQ以及电话与贷款客户进行沟通，在催款过程中难免会出现言语不当或者私下红包转账等情况
- 管理人员如何保障贷后人员业务合规性，以及发现问题可迅速定位人员进行处理，并保障配发设备的专机专用



指掌易方案价值与优势

- 技术先进性，业界领先的VSA技术可实现对业务应用的细粒度化内容审计；
- 功能全面性，提供完整的设备、应用、合规等方面的管控能力；
- 良好的合作伙伴关系，与终端设备厂商深度适配。



指掌易解决方案

- 设备管理：提供标准完整的设备资产管理、设备功能限制管理以及定位管理功能；
- 应用管理：提供应用黑白名单管理能力以及专用的企业应用商店，办公应用可静默安装；
- 上网行为管理：提供URL黑白名单管理以及URL访问记录审计功能，有效保证专机专用；
- 内容审计：支持对手机通话记录和短彩信记录的审计，并可对常用社交类工具的聊天文字、图片、语音、视频、语音通话等实施内容审计；支持针对常用社交类工具的红包及转账审计，并可设定额度进行告警，有效规避业务人员私下违规交易。

安信证券 – BYOD移动办公



客户背景介绍

安信证券是中国证券行业中的领先企业，为持续保持企业竞争力，安信证券一直在使用最新的信息化技术提高效率，驱动业务增长。早在2009年，安信证券就统一配发黑莓手机，实现安全的手机移动办公，并收到了良好效果。为了提供优异的用户使用体验，充分利用移动办公价值，安信证券也希望实施BYOD战略，但同时也希望能够继续保证业务数据的安全性，防止敏感信息外泄。



客户需求痛点

BYOD场景下，鉴于应用产品的标准性以及终端设备的差异性，仅靠移动办公应用自身很难在保障用户体验一致的情况下，实现移动办公门户与个人应用及数据的隔离，也无法提供与公司内部VPN安全通道的无缝集成，因此需要一套移动安全平台，在移动设备与移动应用之间，解决差异性和安全性的问题



指掌易方案价值与优势

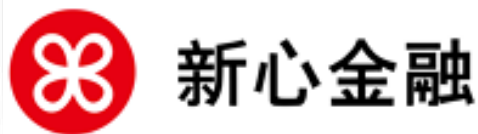
指掌易VSA技术先进，对移动设备适配率高、移动应用兼容性强，应用级数据防泄露策略完整并可细粒度化管控，完全满足BYOD场景下保护业务数据安全、保障用户使用体验的需求。



指掌易解决方案

- VSA技术隔离个人和办公区域，并为应用提供数据加密和防泄露保护，如禁止复制/粘贴、禁止截屏、禁止分享等；
- 使用VSA技术预置应用级VPN通道，为办公应用自动连接企业后台，对办公数据进行加密传输；
- VSA技术对移动设备系统和型号、移动应用类别和版本超级兼容，提供一致的用户体验。


金融行业其他成功案例




谢谢观看！



北京指掌易科技有限公司

 400-898-7798

 指掌易科技

 info@zhizhangyi.com

 北京市海淀区中关村软件园8号楼华夏科技大厦3层

www.zhizhangyi.com