奇安信

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

远程办公安全风险分析及解决方案

陈志华

广东分区技术总监

2020-02-19　　广东省网络空间安全协会

公司概况

奇安信 BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

◆**奇安信集团是中国最大的网络安全公司之一，**专门为党政军企金融等领域提供企业级产品、技术和服务。在“数据驱动安全”理念下，奇安信构建了国内最大的政企安全大数据资源，在大数据安全技术、攻防对抗技术、终端防护技术等领域具有压倒性优势。奇安信的前身为360企业安全集团，2019年4月29日，第二大股东360公司退出，奇安信开始以独立品牌发展。5月10日，中国电子信息产业集团以37.3亿战略入股成为第二大股东，奇安信正式成为网络安全“国家队”。 5月31日完成股改，更名为奇安信科技集团股份有限公司。2019年底成为冬奥会唯一指定的网络安全厂商。

◆**奇安信三年创下三座高峰：**

- 公司价值高峰：两年融资到账50亿
- 增长速度高峰：2016-2018年三年的营业收入的年复合增长率超过90%,2019年订单额增长60%。
- 团队规模高峰：员工人数超过8000人，成为了中国人员规模最大的网络安全企业。

◆**奇安信的使命、愿景和价值观**

- 使命：让网络更安全，让世界更美好
- 愿景：成为全球第一的网络安全公司
- 价值观：客户优先、创新优先、协同优先、当责奋斗、正直诚信、拥抱变化

全民战“疫”，远程办公需求爆发

奇安信

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

- 应用系统远程访问
- IT系统远程运维
- Email、即时通信
- 视频会议
- 资料共享

……

远程办公的场景分析

1. 远程接入办公场景 （SSL-VPN、VDI）　2. 移动办公场景

远程接入，安全迎来“大考”

奇安信

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

传输安全风险

- 数据私密需保障
- 加密算法要合规

身份安全风险

- 单一认证强度低
- 静态口令易破解

访问权限风险

- 接入用户规模大
- 权限控制难精细

接入终端风险

- 远程终端带病接入
- 移动终端风险加剧

恶意行为风险

- 访问行为合规审计
- 异常行为实时监测

奇安信紧急部署启动疫情防控支援工作

奇安信 BEIJING 2022
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

- **1月25日奇安信成立疫情“支援团”，7×24小时为疫情防控信息化系统提供安全服务,根据防控需求提供免费、定制化产品和服务**

免费援助提供对象:

在武汉及疫情防控压力较大区域的相关指挥部门或政企、医疗机构，因抗击疫情所需的IT系统安全防护和协同指挥平台（含软件、硬件及应急服务），都将成为免费援助的对象。

免费援助产品及服务:

1、应急协同与指挥平台（蓝信）
2、终端杀毒（天擎）
3、自适应广域网组网系统（SD-WAN）
4、网站云监测（全球鹰）
5、网站云防护（安域）
6、SSL VPN（远程安全接入）
7、远程在线支持服务（7×24）
8、现场应急服务（7×24）

免费援助保障时间:

本次免费援助时间为自1月26日起，至国家宣布疫情结束为止。

免费援助热线:

凡符合免费援助条件的单位，可随时拨打“支援团”7×24小时免费服务热线：4008136360-6，寻求援助支持。

奇安信为火神山、雷神山医院捐赠全套安全产品

奇安信从1月25日就成立了疫情防控支援团，2月3日前，共计200多位员工奔赴80多个客户现场，另有900多位员工提前到岗，为防控疫情而进行网络安全保护工作。2月3日8000+员工全面复工，启动远程办公方式支持全国各条战线抗疫行动。

目前已为重要的新闻广播媒体系统提供专项的安全防护和专家值守服务，为全国200多家医疗机构(医院、卫生院及卫生健康委员会等)、600多个重要系统提供云端实时监测和防御，并为相关网站提供必要的安全防护。

向全国19个省、市、自治区，100多家医院和疾控等疫情防控一线单位捐赠专业设备和安全服务。截至目前，奇安信和上述地区相关单位达成的意向捐赠金额累计已经达到5000万元。

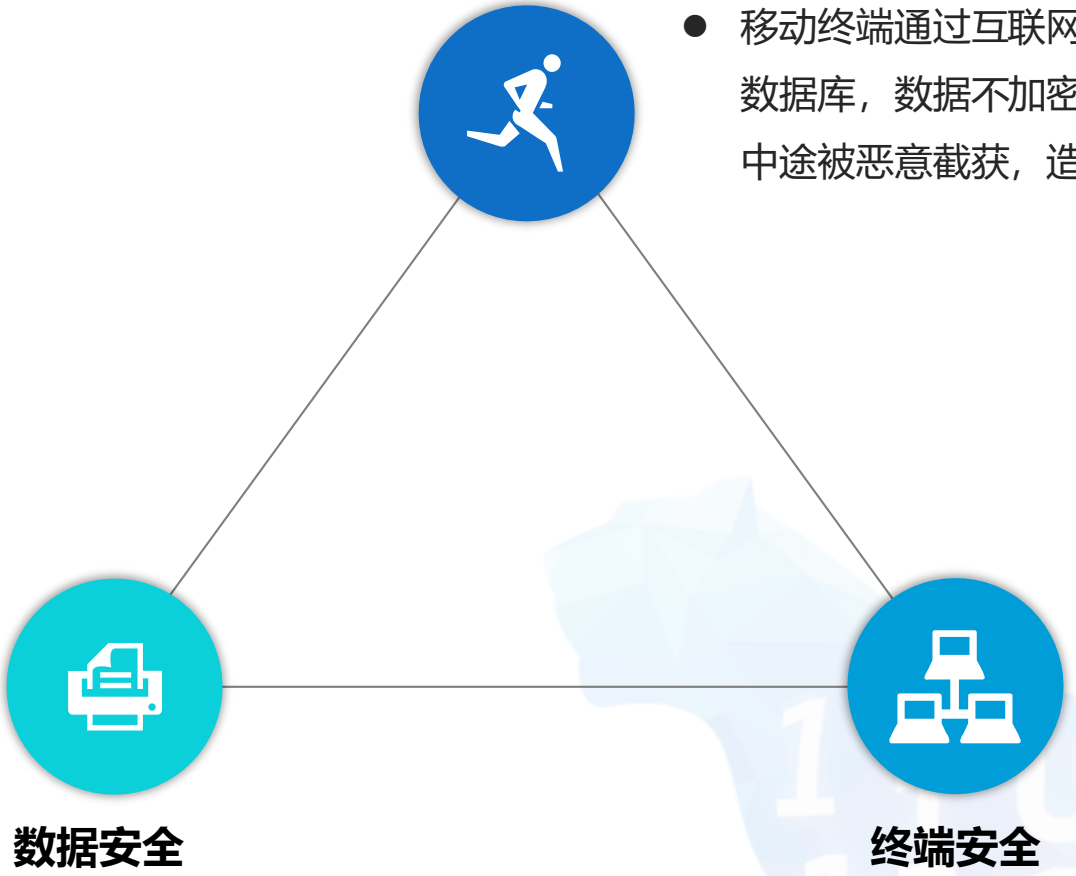
奇安信

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

1

安全远程接入办公

移动办公面临的安全挑战

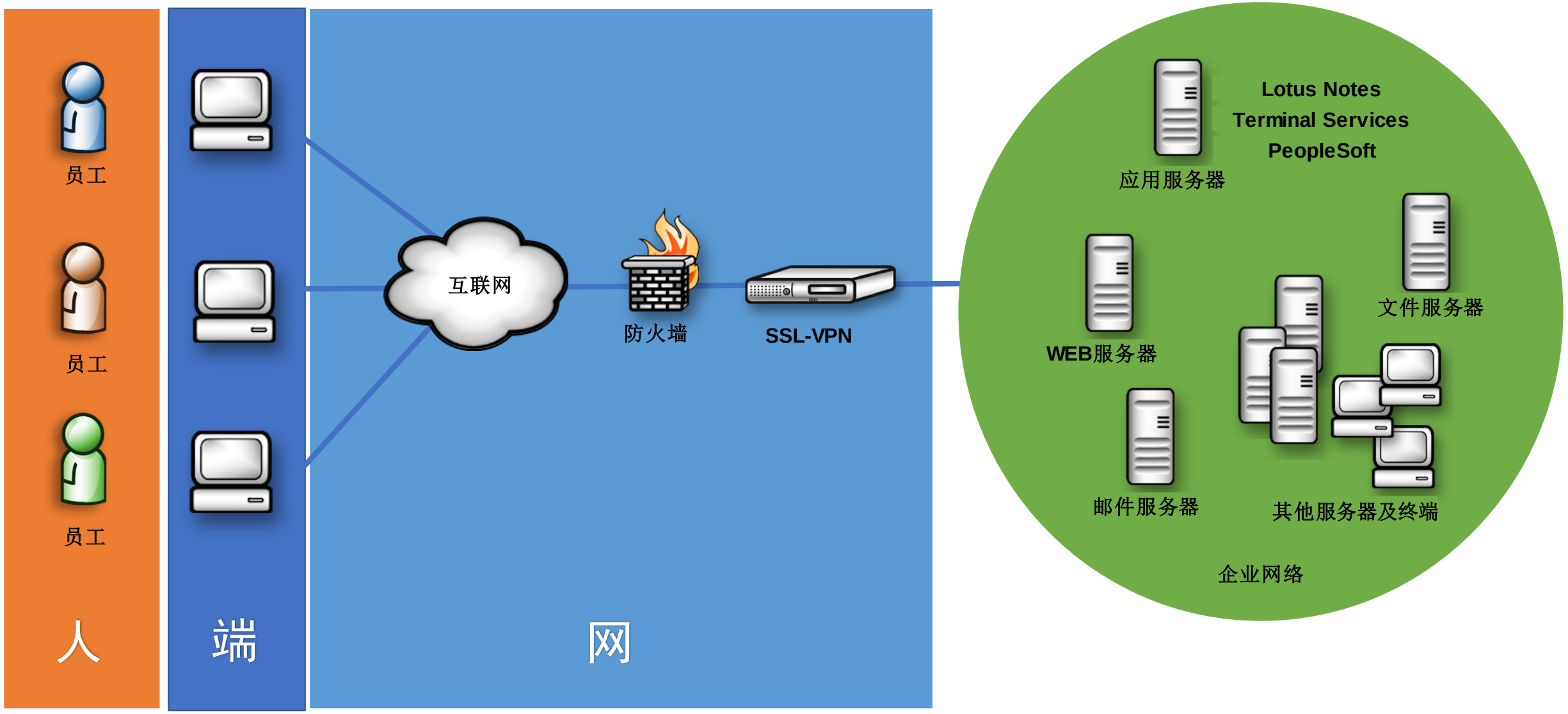


- 移动终端通过互联网传输数据到与内部数据库，数据不加密的情况下，很容易中途被恶意截获，造成大量数据的泄漏

- 数据终端存储未加密易泄漏
- 数据在使用过程中存在风险
- 数据存在截屏、拍照外发的安全风险
- 业务系统本身安全问题存在安全风险

- 个人终端无法合理管控
- 个人终端五花八门、风险不可知
- 随便连接恶意WiFi
- 终端漏洞无法判断
- 病毒、木马入侵没有安全监测系统
- 不法分子利用终端做跳板入侵内网

SSL-VPN场景安全风险分析



SSL VPN远程办公场景的需求分析

奇安信 BEIJING 2022
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

人	正确的人	强认证 （动态令牌、生物识别等）	行为及安全状况分析
端	安全的端	病毒、漏洞、数据防泄密、安检合规	
网	可信的网	隧道加密及访问控制	

多维保障远程接入安全

奇安信

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

身份安全

- 多因素认证
- 生物识别、设备指纹等动态认证方式

传输安全

- 高强度加密算法、商密算法
- 业务、非业务数据隧道分离

权限控制

- 基于角色的细粒度访问控制
- 基于应用的精细化访问控制

终端安全

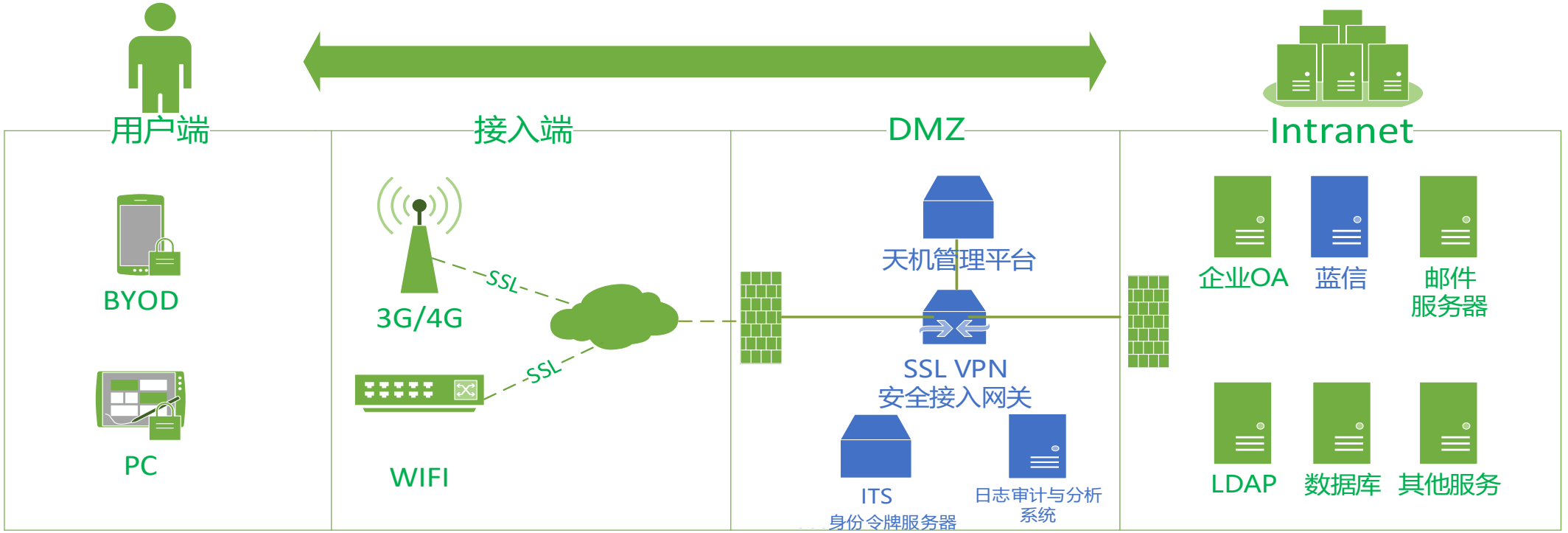
- PC终端安全一体化
- MDM移动安全管理

行为审计

- 访问日志全局审计
- 异常行为建模分析

奇安信安全远程办公解决方案

奇安信 | BEIJING 2022
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022



安全客户端

奇安信ID
客户端

奇安信 VPN
客户端

天擎
终端安全管理系统

天机
移动终端安全管理系统

接入管理中心

传输加密
身份认证
准入控制

SSL VPN
安全接入网关

终端数据同步

天机
管理中心

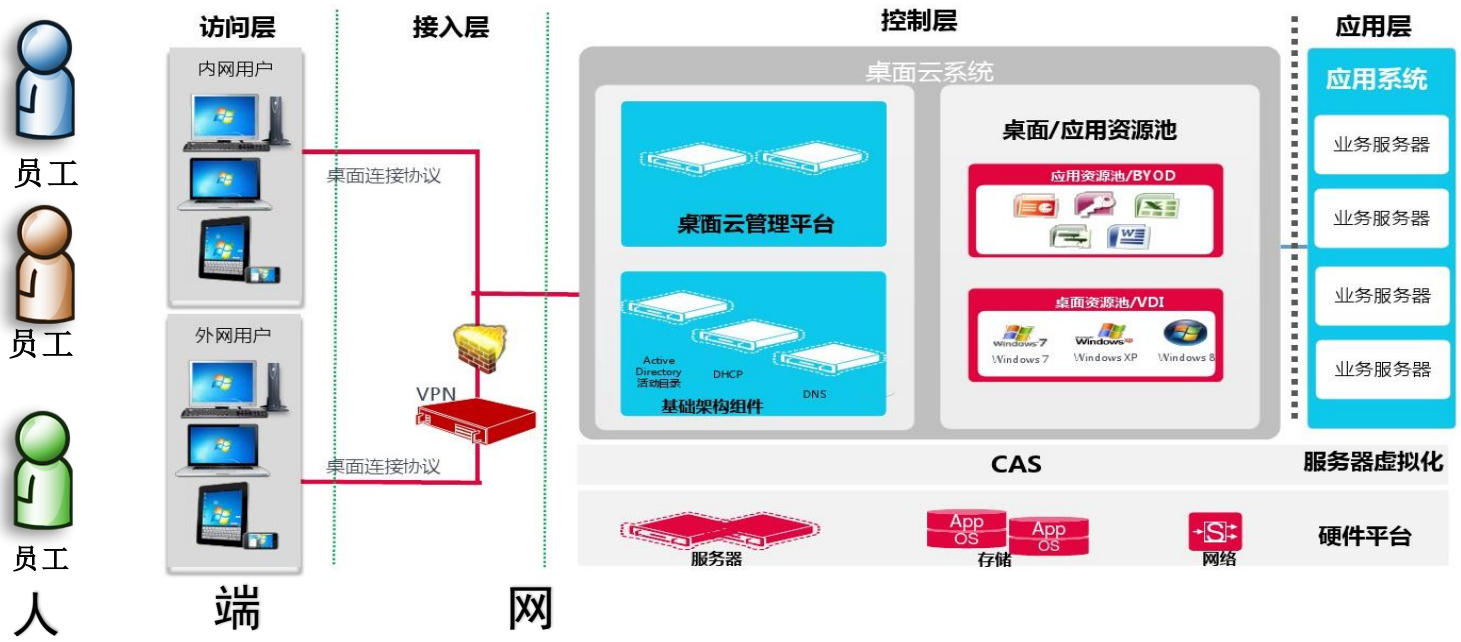
终端管控
沙盒技术
杀毒引擎

数据中心

蓝信中心
安全邮件
系统中心

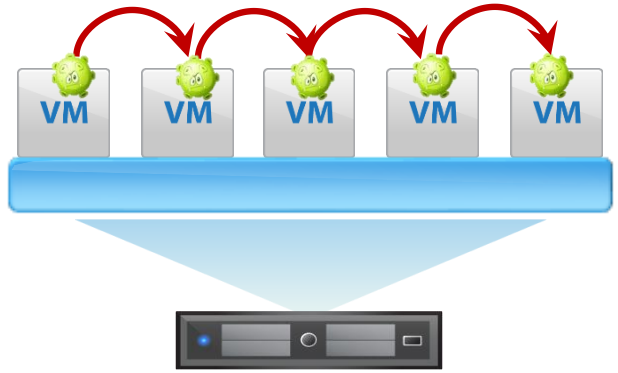
企业OA系统

VDI场景安全需求分析



桌面云是远程办公的利器，具备方便快捷，快速恢复的优点，但仍存在相关安全风险

- 感染病毒、勒索软件等恶意程序，导致文件被破坏和加密
- 恶意程序利用虚拟化特性在东西向快速传播扩散

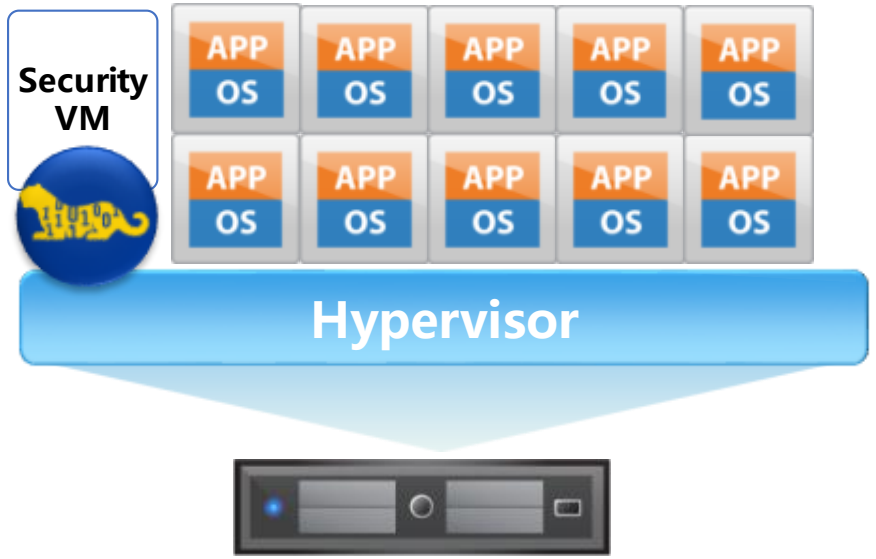


病毒会在虚拟桌面之间快速传播

低资源消耗的虚拟桌面无代理防护

虚拟化安全产品特性与优势：

- 以安全虚机或与Xenserver、KVM深度结合无代理方式部署，
  - 部署、回退快速简单，管理便捷
  - 资源占用小，用户体验好
- 强大杀毒引擎，对所有虚机恶意代码的及时发现和落地查杀，安全无死角，防止恶意代码在网内东西向传播扩散
- 防火墙，实现虚机微隔离
- IPS，抵御各类网络攻击，并可实现虚拟补丁作用



支持桌面云系统（均获得厂商官方认证）

vmware **Horizon、View**

CITRIX **Xendesktop**

HUAWEI **FusionAccess**

产品选配

奇安信 BEIJING 2022
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

解决方案	产品	主要功能	形态与部署
安全远程接入办公	SSL VPN 安全接入网关	提供专用加密隧道，保证通讯传输安全，并执行细粒度、精细化访问控制，终端安全审查	硬件，旁路部署于企业网络外联区
	奇安信 ID	提供基于生物识别及设备指纹的动态验证口令，实现多因素认证	客户端：软件，安装于远程接入用户手机 管理端：硬件，部署于企业网络运维区
	天擎	统一防护策略：终端病毒防护、系统漏洞修复、安全策略有效执行； 数据安全震慑：终端文件水印、外发监测； 内外网全程审计：文件访问操作审计记录、文件打印刻录审计、文件数据外发审计。	客户端：软件，天擎客户端 控制中心：软件，对于客户端和准入进行策略配置。 NAC:硬件，部署于企业网核心交换处。
	日志审计与行为分析	日志收集、行为分析、网络安全状态分析等	管理端：软件，部署于企业网络运维区，需收集SSL VPN、认证、终端防护等相关日志
	虚拟化安全管理系统	为虚拟桌面提供无代理的防病毒、防火墙、IPS、应用管控的功能	客户端：软件，以安全虚拟机(vmware)或部署于Xenserver、KVM虚拟化层中； 管理端：软件，部署于企业网络运维区
	天机	杀毒、数据防泄漏、水印、MTP移动威胁防御、强广管控、SSL VPN、应用套件、可信应用商店、新一代应用沙箱等	移动端：软件，安装于远程接入手机 管理端：软件，部署于企业网络运维区
	蓝信	即时通讯、电话会议、视频会议、考勤、邮件、OA、行政审批、工作日志等	客户端：软件，安装于远程接入手机 管理端：软件，部署于企业网络运维区；或使用SaaS服务

2

移动终端面临新威胁

移动安全威胁事件一

WhatsApp-海外版微信

WhatsApp指责以色列公司NSO攻击其软件，从而对中东等地的持有不同政见的个人、记者、维权人士进行监控，获取重要数据信息。

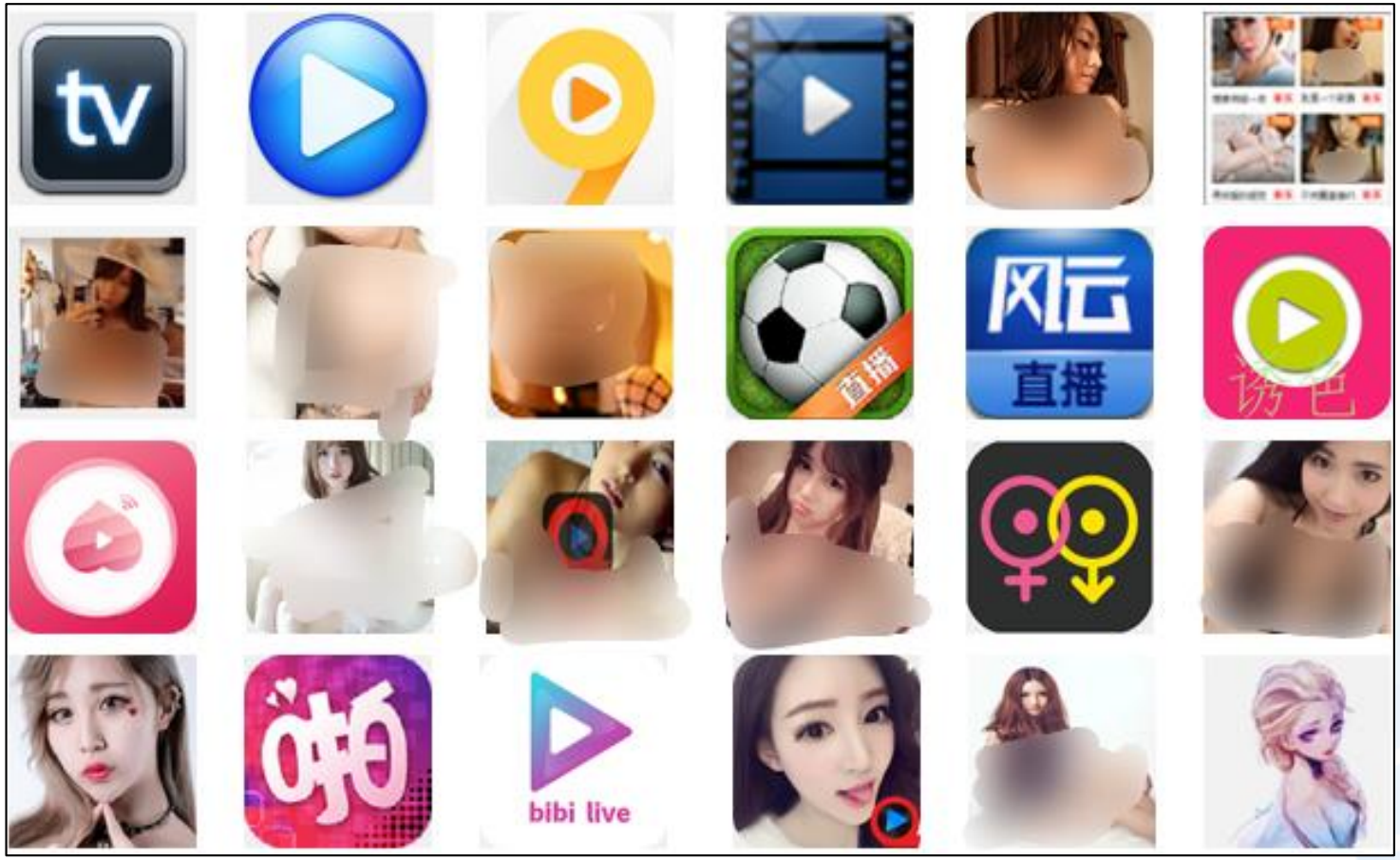
WhatsApp表示，其经过了半年的调查，发现黑客利用其向约1400部手机发动攻击，窃取宝贵的信息。

移动安全威胁事件二

阿联酋，是一个禁用诸如WhatsApp和Skype之类的聊天APP的国家，因此ToTok的出现引领了一股下载风潮。但据熟悉机密情报评估和对该应用程序及其开发者进行调查的美国官员说，ToTok实际上是一种间谍工具。阿拉伯联合酋长国政府使用它来尝试跟踪将其安装在手机上的人们的每一次对话，动向，关系，约会，声音和图像。

ToTok

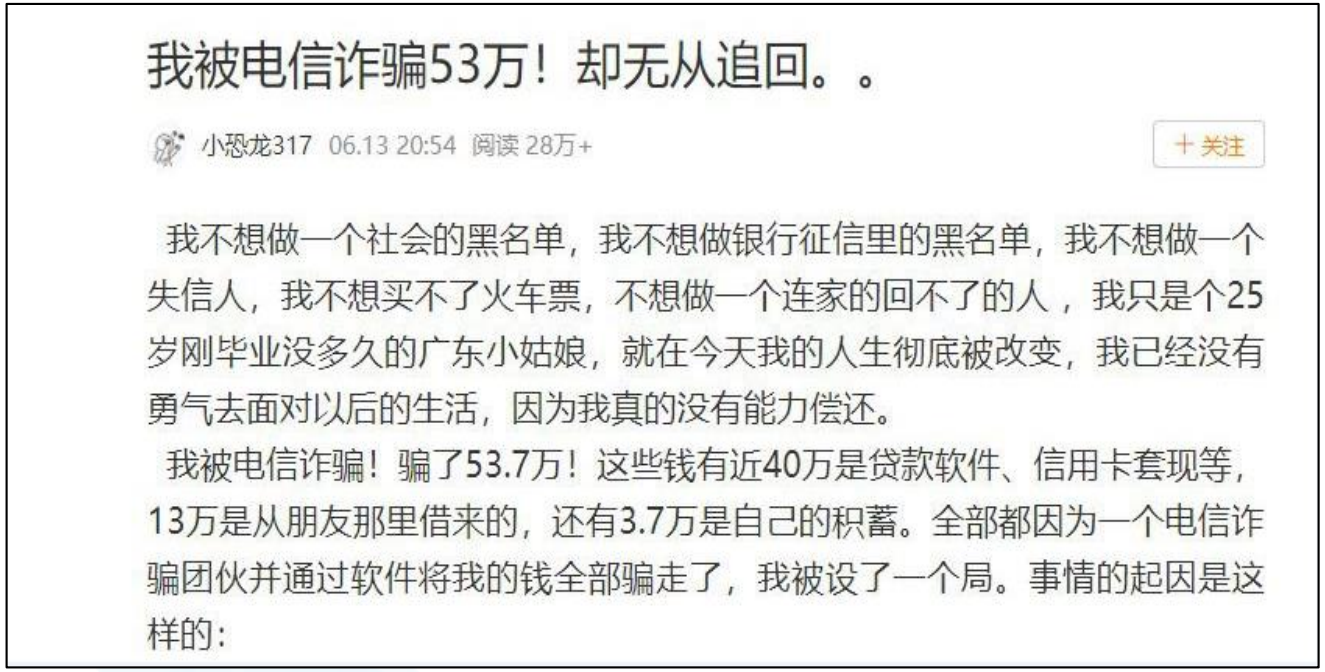
移动安全威胁事件三--国内常见



色情软件常见图标

色情黑色产业近几年在移动应用端异常猖獗，其产业链也已经非常成熟。移动互联网近年来发展迅速，色情产业传播方式也更为多种多样。例如打着视频直播的名号，仿冒正规播放器，甚至通过名目张胆的图标诱骗用户点击的色情软件，以此诱骗用户消费、诱骗用户赌博、大量推送广告牟取利润等。通过色情产业还催生了更多的违法犯罪的行为，给社会带来了巨大的危害，给用户带来了财产损失。

移动安全威胁事件四--国内常见



我被电信诈骗53万！却无从追回。。

小恐龙317 06.13 20:54 阅读 28万+ ＋关注

我不想做一个社会的黑名单，我不想做银行征信里的黑名单，我不想做一个失信人，我不想买不了火车票，不想做一个连家的回不了的人，我只是个25岁刚毕业没多久的广东小姑娘，就在今天我的人生彻底被改变，我已经没有勇气去面对以后的生活，因为我真的没有能力偿还。

我被电信诈骗！骗了53.7万！这些钱有近40万是贷款软件、信用卡套现等，13万是从朋友那里借来的，还有3.7万是自己的积蓄。全部都因为一个电信诈骗团伙并通过软件将我的钱全部骗走了，我被设了一个局。事情的起因是这样的：

仿冒软件一直存在，恶意作者小到通过仿冒当下流行的APP，诱骗用户点击推送广告、推送软件以此获利；大到仿冒银行APP，仿冒第三方支付软件，窃取用户财产，进行诈骗等。2019年我们捕获到了大量的仿冒恶意软件，其中影响较大的有：仿冒银监会客户端，成功诈骗53万的电信诈骗事件；

移动办公过程中移动业务面临的问题

奇安信

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

应用被动态调试

0Day攻击

代码注入

系统ROOT

恶意广告

HOOK攻击

程序被逆向

业务非法访问

文件被篡改

手机丢失

账号被盗

权限被滥用

缺陷配置

病毒木马

应用漏洞

恶意连接海外

系统漏洞

App被破解

钓鱼网络

中间人攻击

虚假WIFI

数据泄露

数据安全

窃听电话

传输安全

屏幕读取

文件泄密

奇安信

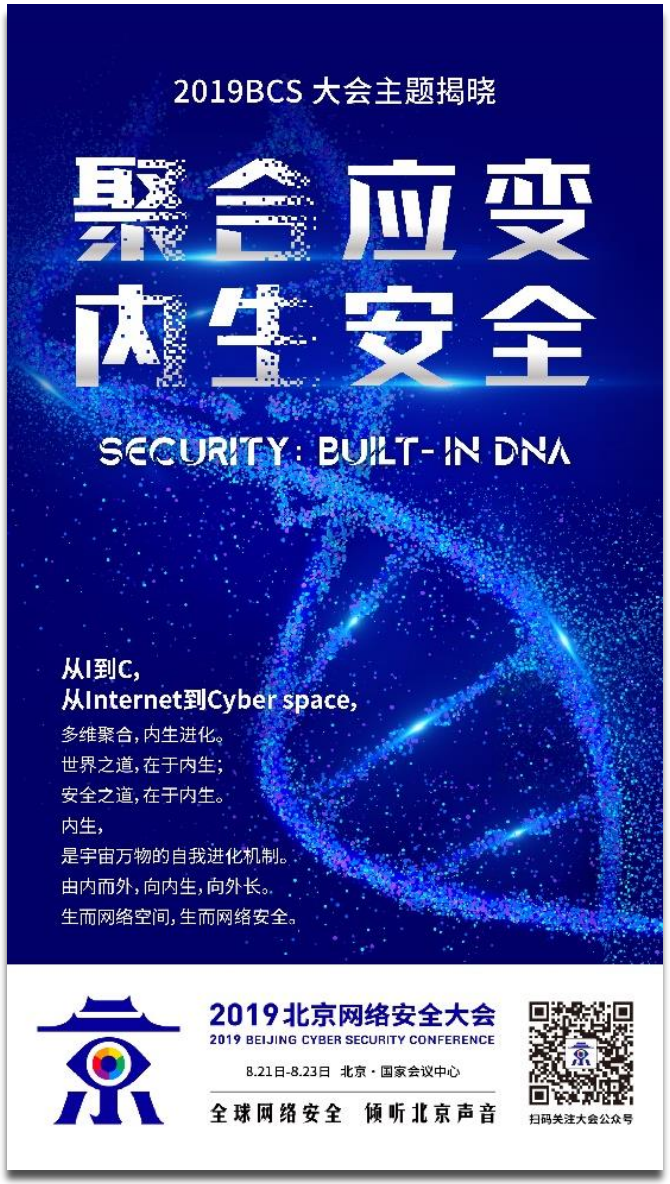
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

3 移动业务安全新战略

移动业务安全新战略-内生安全

奇安信

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022



内生安全是产业变革的共赢选择

奇安信 BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

构建与业务融合的多重、多维度内生安全防御体系

围墙式安全防护

依赖于基础设施

内生安全

固有安全性

内生安全体系特征之一：“免疫功能”

一个自适应的安全系统

网络被攻破，就像人体被病毒和细菌入侵

免疫系统的作用，调动防御力量，消灭病菌

免疫系统崩溃的人，即使生活在无菌室里，也活不过120天

即使是网络被攻破也能保证业务安全

- 一般网络攻击：自我发现 自我修复 自我平衡
- 大型网络攻击：自动预测 自动告警 应急响应
- 极端网络灾难：关键业务 不中断

内生安全体系特征之二：“内外兼修”

奇安信 BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

一个自主的安全系统

完全依靠外在力量，建立不了具有免疫功能的安全系统

因为无论外部检测技术有多高明，都无法感受内部细胞遇到的困难

中医的望闻问切，“问”是关键环节；西医的化验和透视手段，目的也是探究内部细胞变化

安全系统与业务系统深度融合

- 只有外部的安全能力，解决不了内部的安全问题
- 只有外生的安全数据，解决不了内部的安全问题
- 只有泛化的安全大脑，解决不了内部的安全问题

内生安全体系特征之三：“自我进化”

一个自成长的安全系统

免疫系统是需要成长的，大人的免疫系统就比小孩强

锻炼身体、适应严酷环境、对抗疾病都会提高免疫力

网络安全体系在不断抵抗攻击的过程中，也会提高防护能力

安全能力伴随业务变化日渐强壮

- 核心是人的进步和成长
- 不锤炼不可能成为强军
- 不断发现问题解决问题

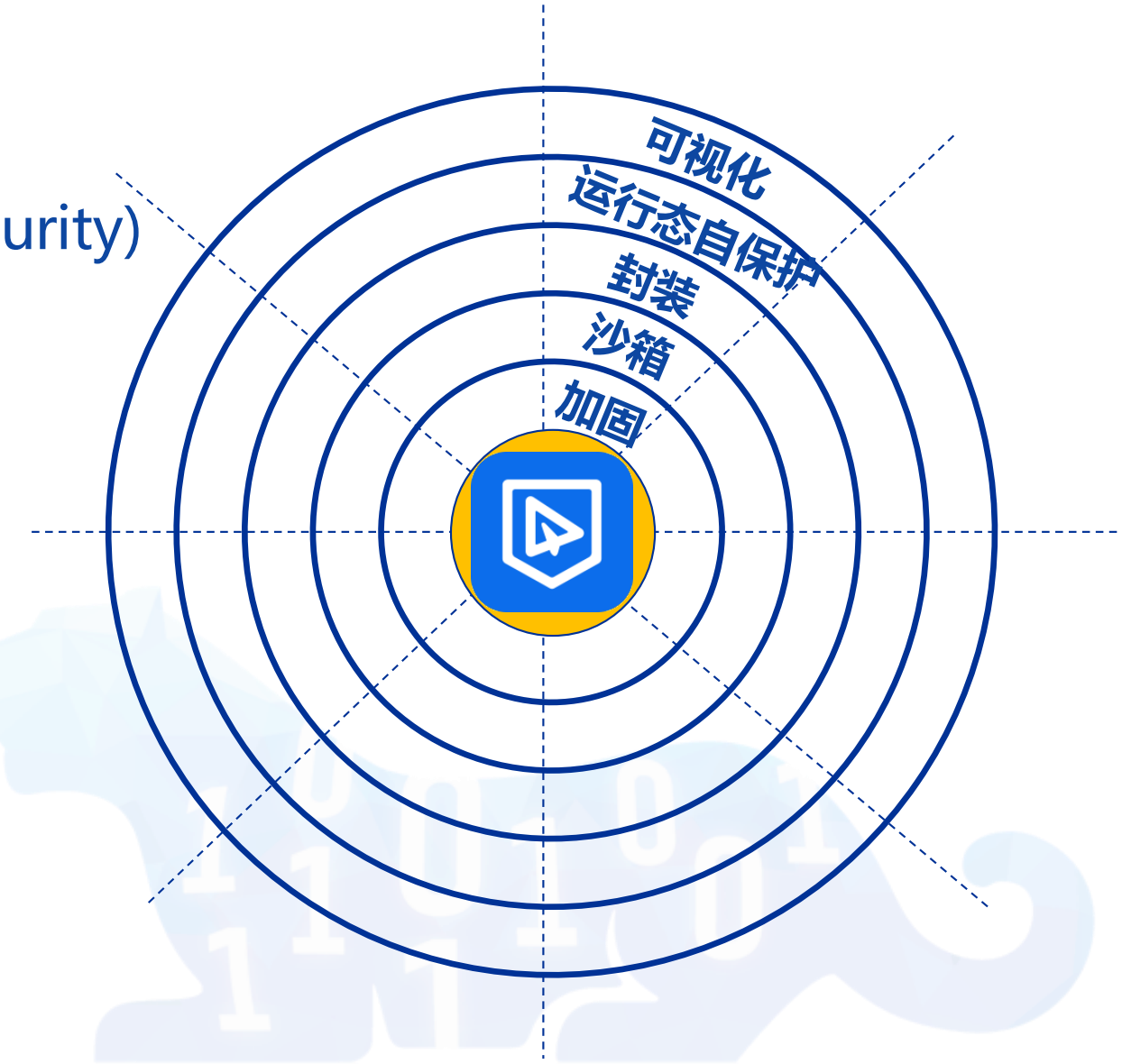
4 移动应用自防护系统

内生安全组件-MIAP

奇安信 BEIJING 2022
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

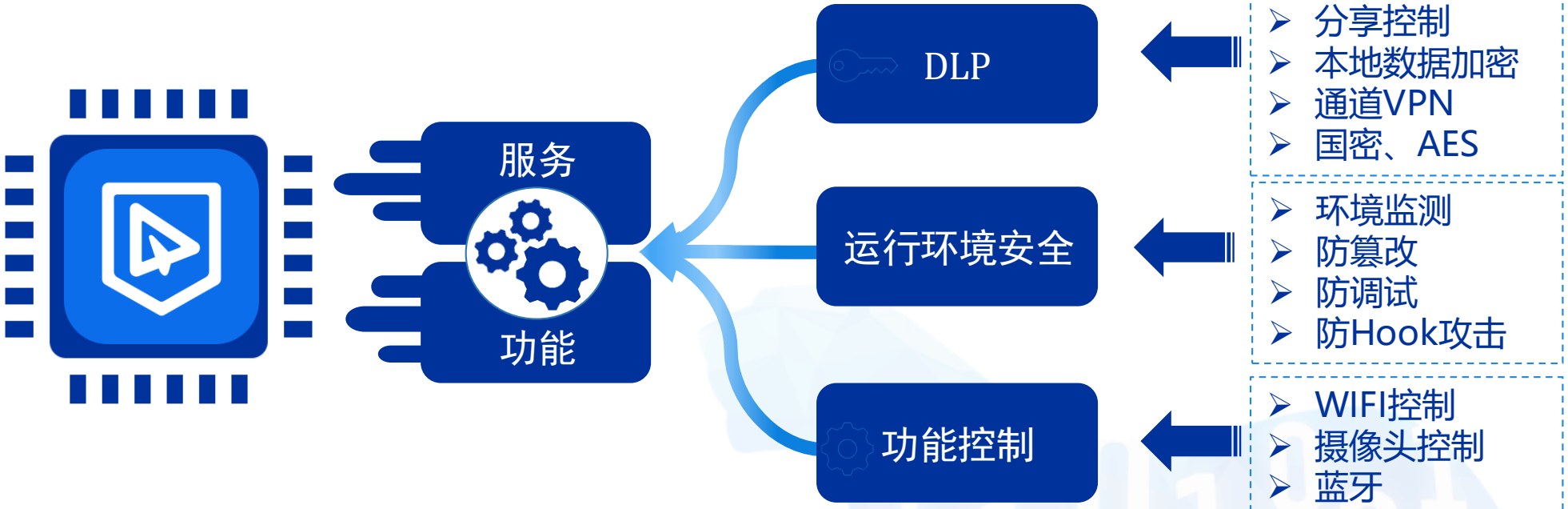
MIAP (Mobile In-App Protection and Security)

通过聚合（加固、沙箱、封装、RASP、可视化等）多种安全技术，将诸多应用安全技术注入到企业App内部，构建企业App内生安全体系，保障企业App的应用安全和数据安全



内生安全实现技术手段-封装技术

代码零改动，聚合多种安全能力



封装后应用与管理平台联动

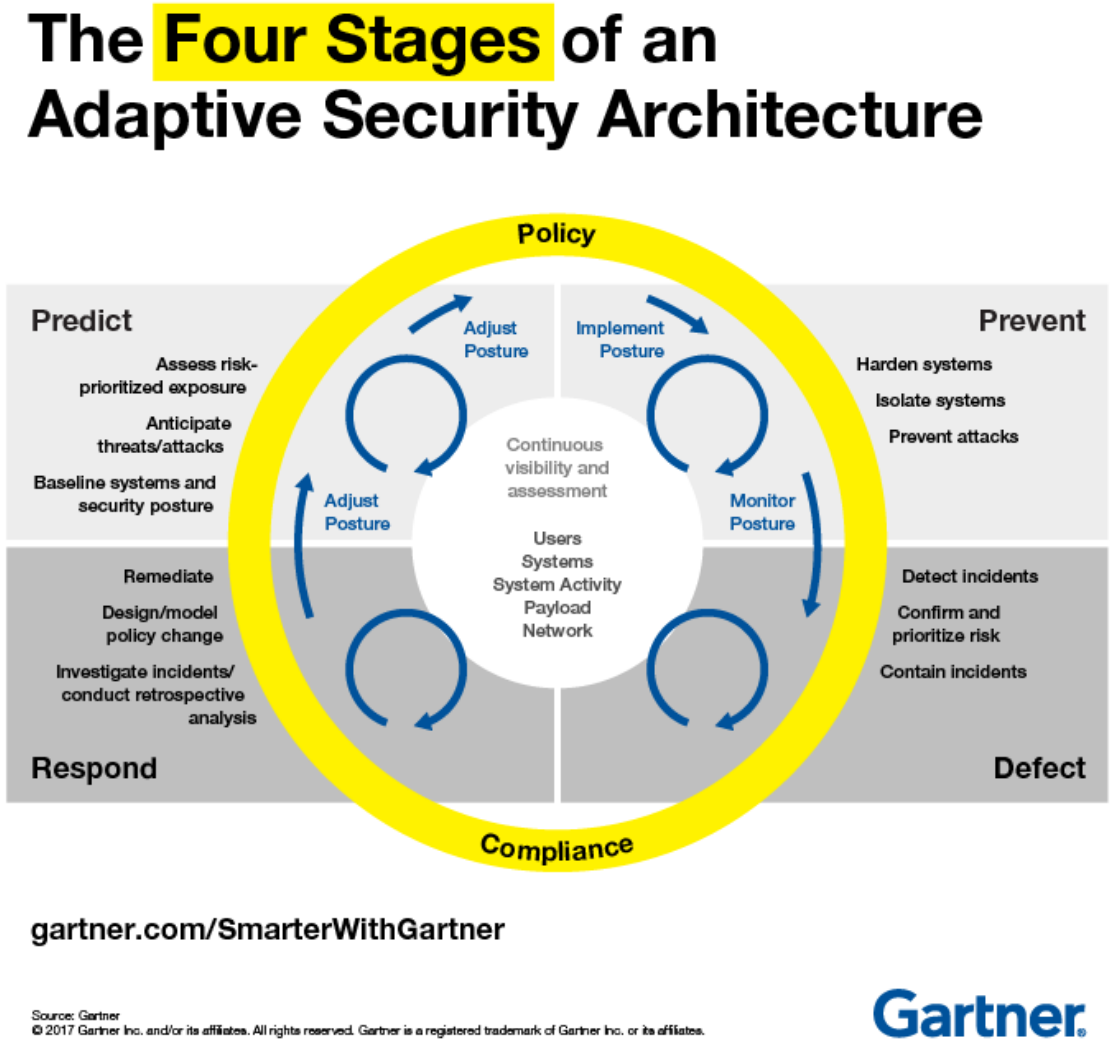
运行态自保护-RASP

运行态自保护

Runtime App Self Protection

将自身注入到应用程序中，与应用程序融为一体，实时监测、阻断攻击，使程序自身拥有自保护的能力。

实现从静态防护、事件驱动，向动态防护、风险驱动、主动防御的转变。



安全能力- 应用加固

奇安信

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

1 有效防止反编译

使用VMP壳代理加载、抽取JAVA代码方法等技术保证原始文件不被反编译

2 有效防止动态调试

运行时根据应用运行功能进行动态回填防止内存dump，通过ptrace进程的手段防止动态调试。

3 稳定性好 兼容性高

独有技术，兼容android 2.3-9.0全部版本以及市面上绝大多数android定制OS系统，亿级C端用户支撑。

安全加固核心价值

奇安信 BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

- Dex 文件 VMP保护
- SO文件加密保护
- LLVM源码保护
- 通讯协议加密SDK

- 主配文件防篡改保护
- 资源文件完整性保护
- 数据文件加密保护
- 签名校验保护

- 防内存截取攻击保护
- 防内存非法读取/修改
- 防动态注入攻击保护
- 防动态调试保护

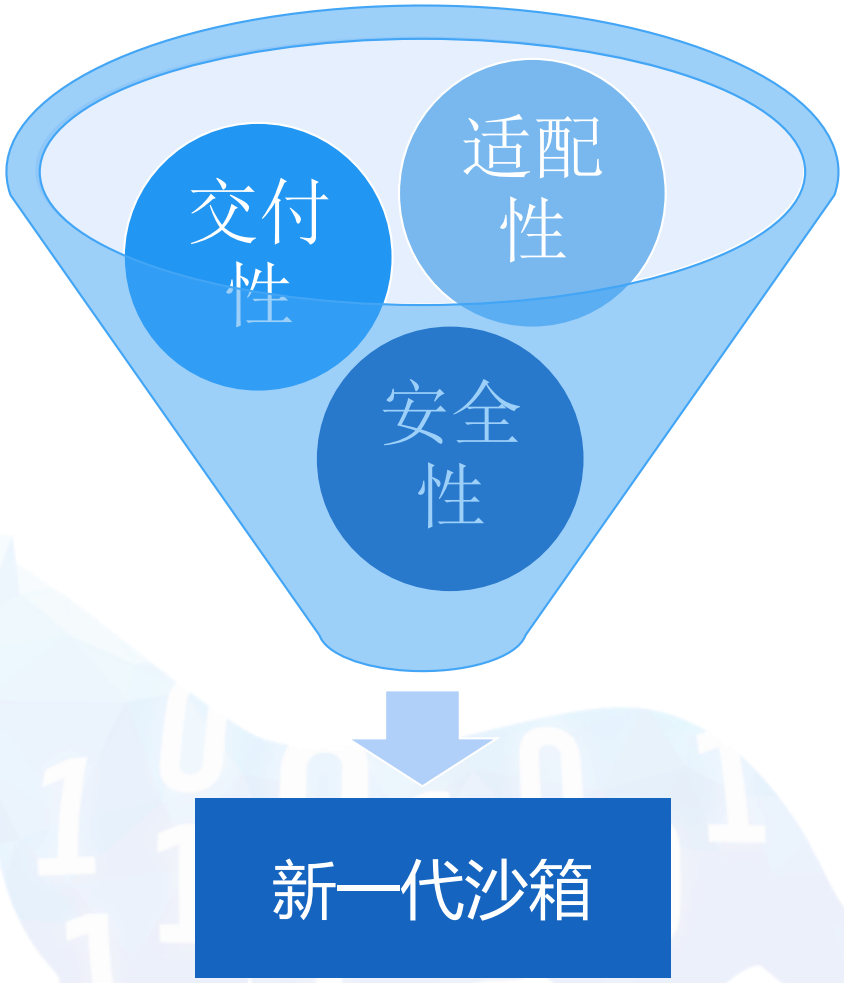
业务应用构建独立沙箱

奇安信

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

自主构建安全可控的虚拟运行环境

- 专利技术保障的新一代沙箱
- 企业应用100%适配，不破坏原始App
- 密钥沙箱，文件加密，Per APP VPN，DLP，访问控制，安全功能一应俱全
- 应用行为，安全审计，一览无余



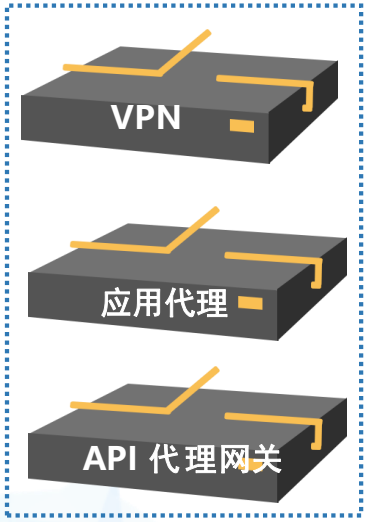
移动应用安全接入

奇安信

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

用于**用户/终端**和**业务应用**之间的安全访问

安全接入



将业务隐藏在网关之后，默认不可见

传输加密

- 专业的TLS传输技术
- 支持国密算法套件
- 防中间人攻击

访问代理

- 业务默认隐藏，强制授权
- 令牌传递，实现单点登录

全量日志

- 访问日志输出到身份分析平台进行风险评估
- 流量可视化

移动业务安全可视化

奇安信 | BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

RASP

设备安全状态 (单位：台)

- 安全：74
- 风险：251

风险状态 (单位：次)

- 运行环境：17
- 应用攻击：51
- 敏感行为：135

运行环境状态 (单位：次)

- 调试攻击：17
- 系统ROOT：0
- 系统篡改：0

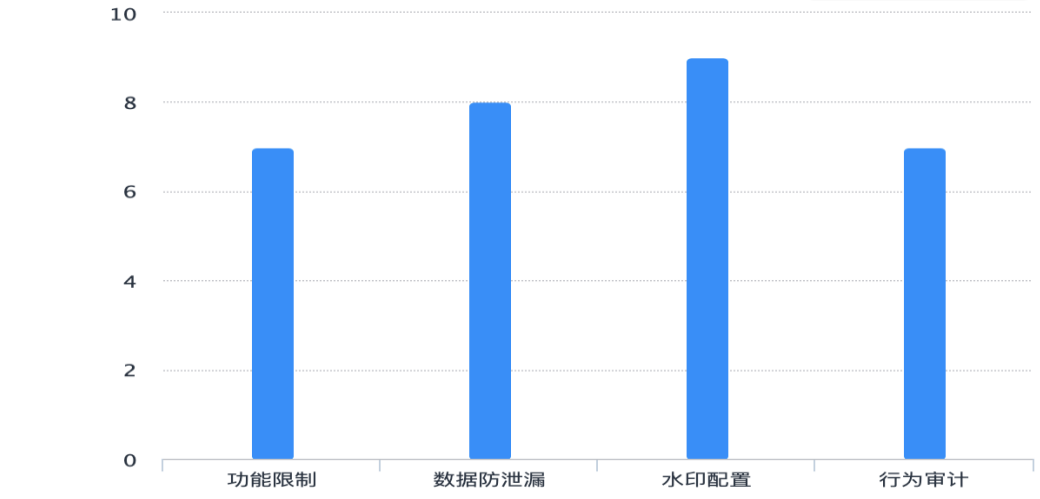
敏感行为状态 (单位：次)

- 读取剪切板：46
- 分享数据：6
- 显示通知栏消息：83

封装加固

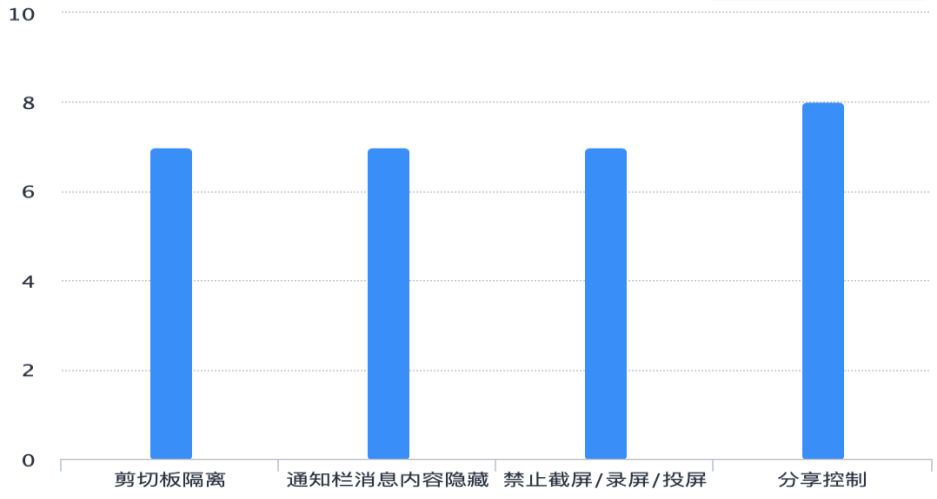
沙箱策略执行情况 (单位：台)

蓝信+



数据防泄漏策略执行情况 (单位：台)

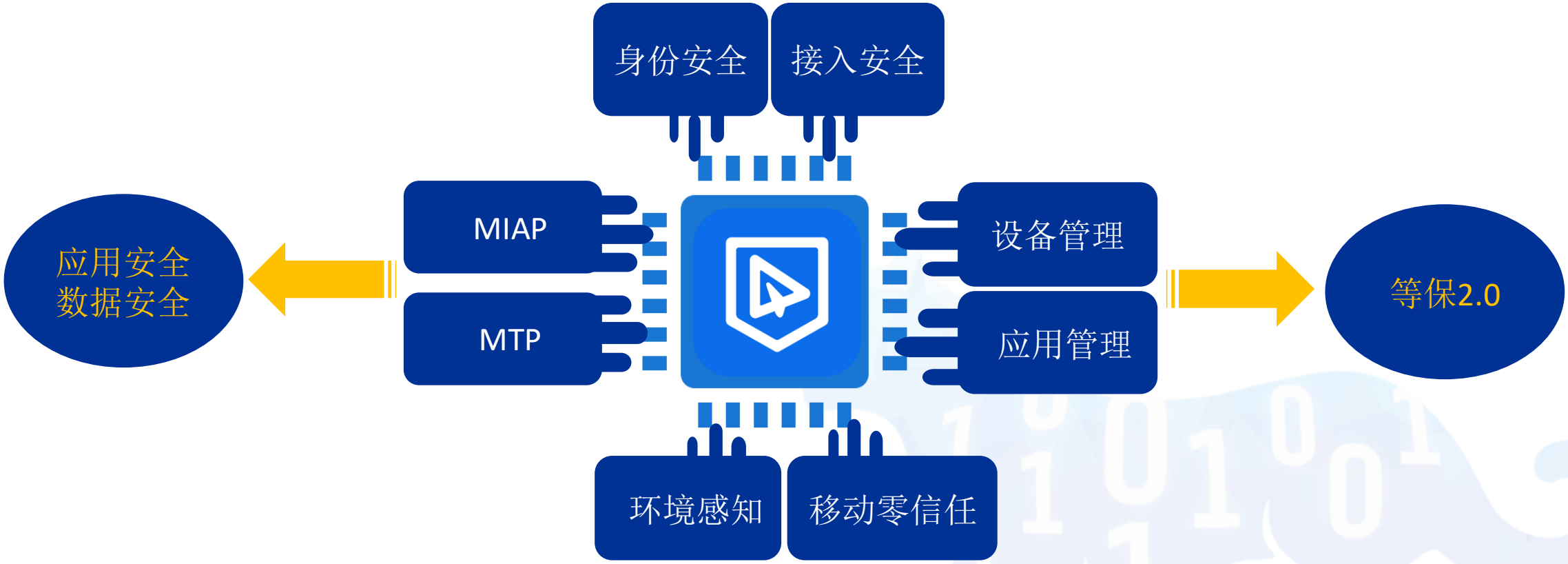
蓝信+



移动业务内生安全立体防御体系

奇安信 BEIJING 2022
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

内置多种安全能力，具备自适应、自主、自成长内生安全特性



客户价值体现

奇安信

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

数据安全

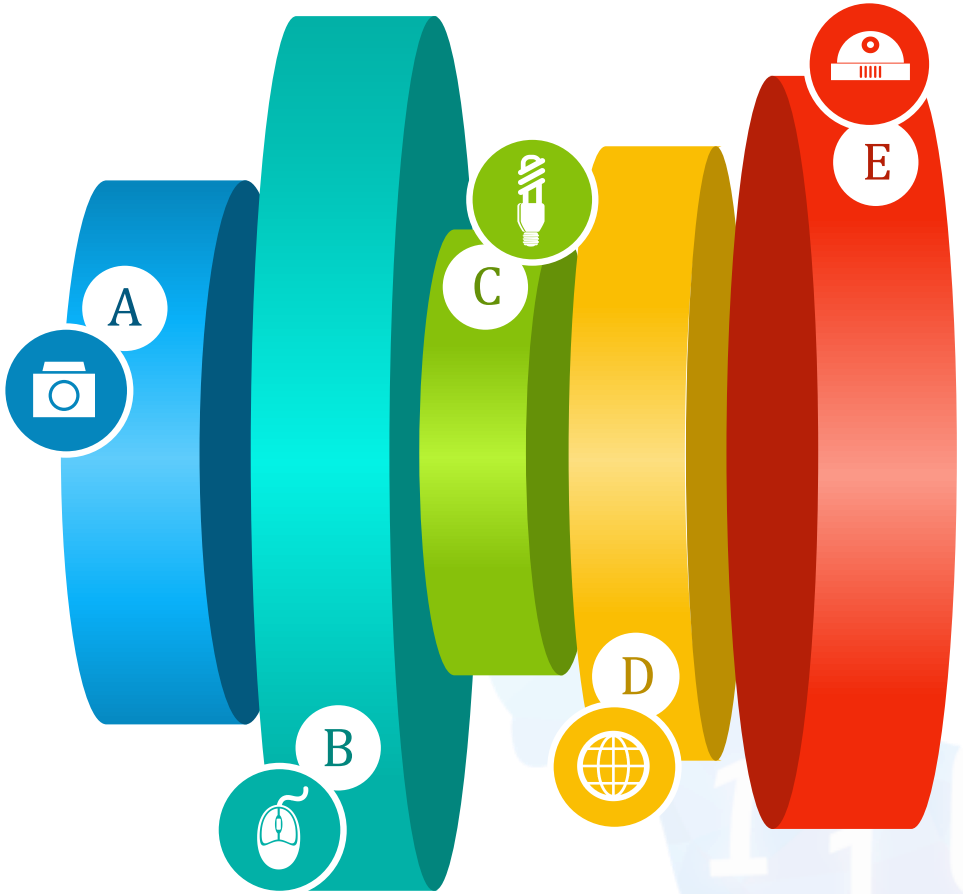
通过安全沙箱、密钥沙箱技术确保移动终端数据安全性

传输安全

通过应用封装技术将安全传输能力赋予业务系统，确保数据传输安全。

应用安全

通过应用封装技术赋予业务应用安全能力，确保应用全生命周期的安全性。



终端安全

通过移动安全防御系统的保护，确保移动终端环境的安全可靠。

体验极致

应用封装不改变原始的操作习惯，工作人员使用简单、方便，带来极佳的用户体验。

移动业务安全整体框架

奇安信 BEIJING 2022
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

移动业务安全框架

安全感知	威胁感知平台	态势感知	威胁情报	
行为分析	用户行为	应用分析	行为审计	
移动零信任	身份安全ITS	访问控制TAC	可信代理TAP	
	移动可信环境感知MTESS			
网络接入	VPN	可信应用代理	API代理	
身份安全	身份安全ITS	多因素认证	SSO	统一认证
数据安全	MIAP	工作区/沙箱	MRSAP	DLP
应用管控	MAM	App全生命周期安全（加固、封装、风险扫描、权限评估等）		
设备管控	MDM	COPE	BYOD	
环境安全	移动威胁防御MTP	系统安全	WIFI安全	App安全
基础能力	管控、沙箱、加固、封装、SSO、RASP、接入、扫毒、感知等			

奇安信

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

THANKS

让冬奥更安全　让世界更精彩