2020北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE

内生安全 从安全框架开始

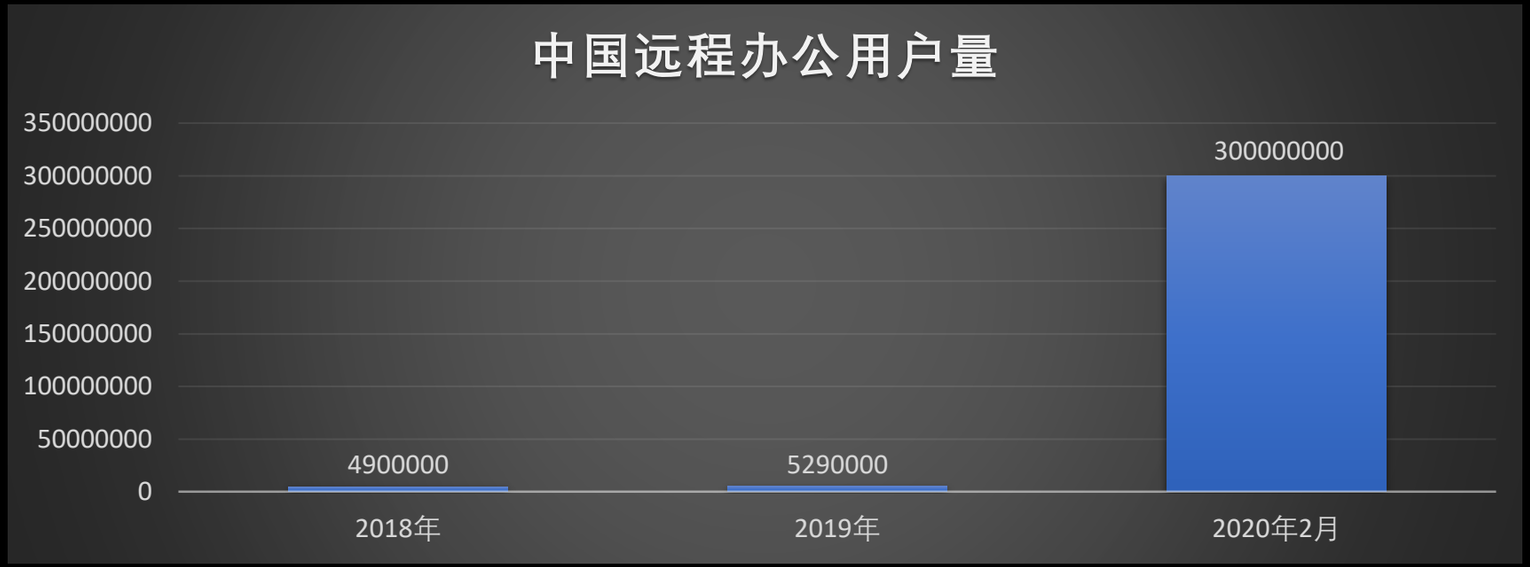
ENDOGENOUS SECURITY:
STARTING FROM AN ARCHITECTURE

2020.8.07-8.16

全球网络安全 倾听北京声音

远程办公正在进化到内生安全时代

蓝信移动　路轶


中国远程办公用户量
350000000
300000000
250000000
200000000
150000000
100000000
50000000
0
4900000
5290000
300000000
2018年
2019年
2020年2月

远程办公 - 效率与风险并存

移动业务的边界从办公室扩散到泛化网络的任意人员、任意时间、任意地点，安全风险同样呈现新的特征

- 更易发生的终端丢失
- 更多样的病毒木马
- 更广泛的外设出口及数据泄露
- 更复杂的身份多样化及冒用
- 更多暴露面的数据传输窃听风险
- 更容易污染植入的APP应用
- 更具移动化特征的业务违规操作

移动安全新趋势

设备/网络•••>应用/数据	管理优先•••>用户优先
➢ 移动端承载越来越重要的企业移动业务应用 ➢ 安全风险从设备/网络层上移至应用/数据层	➢ 移动办公属性决定了PC管理模式存在不足 ➢ 用户体验直接决定移动化项目的成败

终端风险 | 接入风险 | 越权风险 | 系统风险 | 应用风险 | 数据风险 | 业务风险 | 管理风险

远程办公正在进化到内生安全时代

传统的安全防护手段局限在内外边界；远程办公面临的威胁要求安全能力构建在业务系统上，从而保证系统能生长出内生安全能力。

业务系统和安全系统泾渭分明的传统格局已无法满足远程办公所面对的日益严峻的威胁，业务系统自身必须聚合安全能力，自身就是具备高安全性的系统。

自主

业务系统具有应对极端网络灾难、保证关键业务不中断的能力；针对一般性攻击和威胁自我发现、自我修复、自我平衡的能力；核心为自动感知、自动告警和应急响应的能力。

自适应

安全能力动态提升。既是数字化转型过程业务系统功能升级，流程再造的时候，安全能力应该能同步提升，也是系统使用者安全相关认知能力的进步和成长，系统与人同步进化。

自成长

系统安全

顶层架构设计

蓝信平台按服务进行拆分，分为多个独立的子系统，包括：接入服务、通讯录服务、消息服务、短信服务、外部联系人服务、开放平台服务等等。各个子系统，都是集群部署方式，不会造成单点故障。

系统集成

蓝信开放平台服务提供了标准的接口能力，组织的办公系统可通过对接蓝信开放平台，可将组织内的系统集成互联在一起，简单、开放、扩展。

系统扩展性

蓝信独立服务的模式，业务的扩展不会影响蓝信的使用，只需要扩展服务或维护某个服务即可。

服务监控

实时对蓝信服务进行监控，故障报警、服务异常报警、流量报警，并能有效组织异常访问

数据安全

自主

蓝信SaaS平台

蓝信公有云平台通过公安部等保三级，申请成功后即时开通。免除客户运维和保障支持

私有化部署方式
客户提供部署资源

私有云托管

在蓝信机房租用独立服务器，保证数据独立，客户拥有服务器所有管理权限。蓝信私有云平台通过公安部等保三级

独立部署

（客户自行租赁第三方云平台或传统服务器部署）

部署在用户指定数据中心，数据存储全部放在客户本地数据中心，客户拥有所有的管理权限

分级部署

部署在各个平台之间的组织可实现管理、业务和人员的横向、纵向挂接。满足政府组织、大型企业组织的统一组织、分散建设的部署要求

业务安全

自主

可见性设置

- 支持高级可见性设置，每个人只能看到被允许看到的通讯录信息

终端数据保护

- 远程擦除蓝信数据，保证不泄密
- 管理员后台删除离职员工，员工数据实时清除，保护数据信息

电子水印

- 标题内嵌文档阅读器，不需要第三方应用打开，文档不流出蓝信
- 客户端全局、文档查看采用个人身份信息电子水印，防止截屏

传播防范

- 可限制普通用户建立群聊、群发的群大小
- 支持设置组织内敏感词
- 支持审核公告内容

信息转出审计

- 所有信息转出蓝信，服务器后台记录，满足审计需求

安全认证

自主

商用密码产品认证证书

证书编号：GM001119920201113

委托人名称及所在地
蓝信移动（北京）科技有限公司
北京市朝阳区酒仙桥中路24号878东区6层

生产者（制造商）名称及所在地
蓝信移动（北京）科技有限公司
北京市朝阳区酒仙桥中路24号878东区6层

生产企业名称及所在地
蓝信移动（北京）科技有限公司
北京市朝阳区酒仙桥中路24号878东区6层

原商用密码产品型号证书批准型号
SHT1834 移动信息传输加密平台（原证书编号：SXH2018302号）

依据商用密码产品型号证书换发。

颁发日期：2020年07月01日　　有效期至：2023年12月16日

证书有效期内本证书的有效性依据发证机构的定期监督获得维持。

牛路宏

国家密码管理局商用密码检测中心

业内唯一通过国密认证

蓝信国密解决方案完全支持且符合国密算法要求（SM2/3/4/9），是业内唯一通过国密认证的移动工作平台产品

信息系统安全等级保护
备案证明

依据《信息安全等级保护管理办法》的有关规定，蓝信移动(北京)科技有限公司 单位的：

第三级 蓝信专属 系统

予以备案。

证书编号：11010517049-00001

中华人民共和国公安部监制

备案公安机关公章

2017年5月17日

公安部等保三级认证

蓝信是国内第一家获得公安部等保三级认证的移动工作平台，率先在移动办公领域引入“安全工作”的理念

等级测评结论

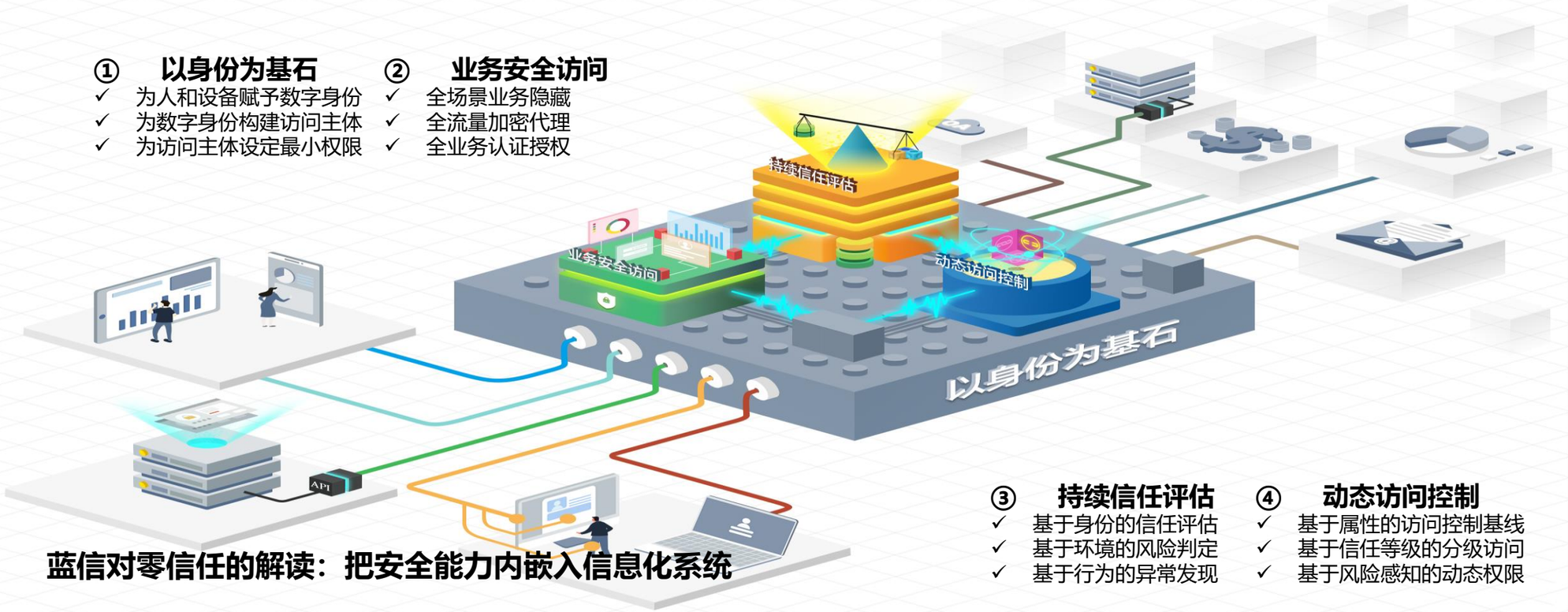
等保2.0三级测评

蓝信SaaS平台，已经通过了等保2.0三级测评

自适应

① 以身份为基石
- ✓ 为人和设备赋予数字身份
- ✓ 为数字身份构建访问主体
- ✓ 为访问主体设定最小权限

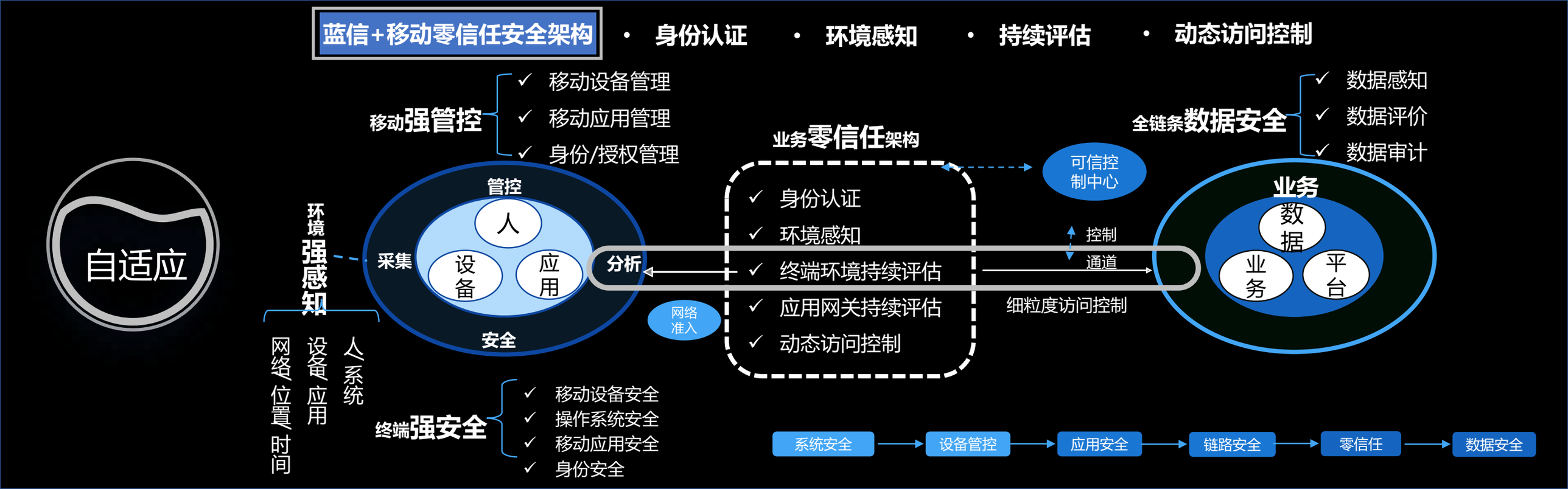
② 业务安全访问
- ✓ 全场景业务隐藏
- ✓ 全流量加密代理
- ✓ 全业务认证授权

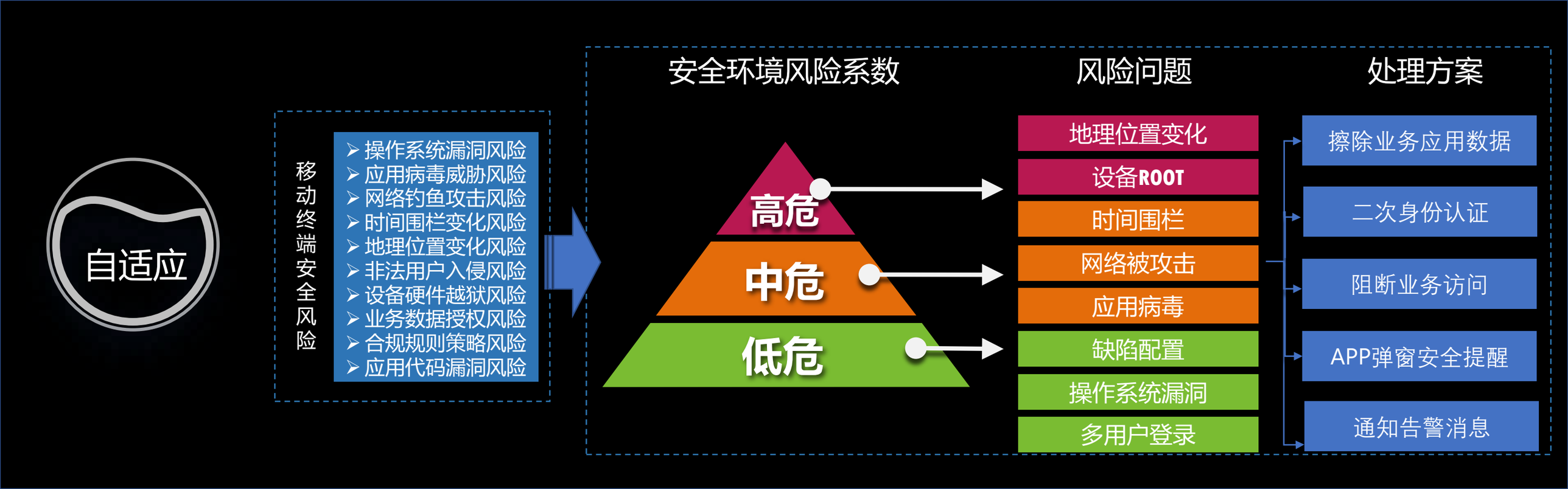


蓝信对零信任的解读：把安全能力内嵌入信息化系统

③ 持续信任评估
- ✓ 基于身份的信任评估
- ✓ 基于环境的风险判定
- ✓ 基于行为的异常发现

④ 动态访问控制
- ✓ 基于属性的访问控制基线
- ✓ 基于信任等级的分级访问
- ✓ 基于风险感知的动态权限


蓝信+移动零信任安全架构
身份认证
环境感知
持续评估
动态访问控制
移动强管控
移动设备管理
移动应用管理
身份/授权管理
全链条数据安全
数据感知
数据评价
数据审计
自适应
环境强感知
人/系统
设备/应用
网络/位置/时间
管控
人
设备
应用
采集
分析
安全
网络准入
业务零信任架构
身份认证
环境感知
终端环境持续评估
应用网关持续评估
动态访问控制
可信控制中心
控制
通道
细粒度访问控制
业务
数据
业务
平台
终端强安全
移动设备安全
操作系统安全
移动应用安全
身份安全
系统安全
设备管控
应用安全
链路安全
零信任
数据安全


自适应
移动终端安全风险
操作系统漏洞风险
应用病毒威胁风险
网络钓鱼攻击风险
时间围栏变化风险
地理位置变化风险
非法用户入侵风险
设备硬件越狱风险
业务数据授权风险
合规规则策略风险
应用代码漏洞风险
安全环境风险系数
高危
中危
低危
风险问题
地理位置变化
设备ROOT
时间围栏
网络被攻击
应用病毒
缺陷配置
操作系统漏洞
多用户登录
处理方案
擦除业务应用数据
二次身份认证
阻断业务访问
APP弹窗安全提醒
通知告警消息

移动业务平台安全保障 - 目标

以蓝信平台为基础，基于自主可控安全技术，深度融合安全与移动办公业务，全面覆盖移动安全各层面，构建满足企业系统级的端到端整体移动安全保障体系，确保移动办公的合规性，充分保障移动办公数据的安全性以及业务连续，基于零信任理念满足移动办公访问的可信性，支撑蓝信移动办公平台为客户提供安全且不失便捷的移动办公服务。

合规

- 等保2.0
- 移动应用建设规范

安全

- 端到端安全防护

可信

- 终端可信
- 业务可信
- 动态访问控制

自主可控

- 底层基础设施

自成长

运营阶段+运营方法

场景挖掘、初期启动、试点推进、全面应用

对应四个阶段，提供相应的系统化运营方法

重保安全保障服务

•7*24小时电话技术支持

•20分钟内响应问题，2小时内问题处理

•节假日、重大事件、突发事件的运维值守服务

总结经验，丰富业务扩展

•总结归纳，完善业务流程；

•制定后续方案；

•分享和扩展更多工作场景。

◆重保、应急处置经验丰富：对于管控机构及相关单位应急响应迅速

支持2018-2019公安部HW行动，为公安部唯一指定即时通讯通报平台

支持2019年10月10日交通部针对无锡塌方事件现场连线，确保部长第一时间获取现场信息

支持2020年1月中国人民政治协商会议北京市第十三届委员会全程会议，为委员履职唯一移动平台

支持交通部、外交部、新华社、中央网信办、水利部等部委客户每年国庆、春节期间的重保服务

支持中国有色、中国铝业等中央企业每年度集团大型会议（移动会务产品支撑+现场重保支撑）

◆ 提供驻场运维、客服等专职保障人员进行服务保障

中央网信办、新华社等专属驻场客服人员

中央网信办、江苏省公安厅、云南省公安厅、河北省公安厅等专属驻场运维人员

疫情加速了远程办公的整体进度。
行业在风口，现实的风险要求远程办公必须向内生安全进化。
业务系统和安全系统的边界消失，逐渐融合，实现自主。
零信任安全架构无缝嵌入业务系统，实现自适应。
平台能力赋能子系统，服务保障赋能人，系统+人共同进化实现自成长。

蓝信

大企业 用蓝信

安全移动工作平台

THANKS