电子政务安全解决方案

2020年6月，在对全国数字政府建设指数的评估结果中，全国数字政府建设指数平均值为51.7，其中14个省（区、市）指数达到平均值及以上。广东省以总指数75.2届全国榜首，浙江、山东、福建、北京位列第2-5名，总指数分别为73.4、71.0、68.5、68.4。

--数据来源：赛迪顾问2020/06

在《国务院关于加快推进全国一体化在线政务服务平台建设的指导意见》国发〔2018〕27号中指出，“建立全国一体化在线政务服务平台安全保障协调联动工作机制，制定完善应急预案，构建全方位、多层次、一致性的防护体系”、“制定全国一体化在线政务服务平台数据安全管理办法，加强对涉及国家利益、公共安全、商业秘密、个人隐私等重要信息的保护和管理，加强政务大数据安全管理”。涉及等保合规、开放数据接口安全和安全运营体系等安全方面的建设需求。
“加快建设国家政务服务平台移动端，接入各省（自治区、直辖市）和国务院有关部门移动端服务资源，提供分级运营、协同联动的全国一体化在线政务服务平台移动端服务”，移动端（APP+小程序）成为主要业务载体。

安全保障能力不足

各地安全防护能力参差不齐，基层平台普遍缺乏全方位、多层次的移动安全防护体系，对接上级政务服务公共入口后成为安全短板。

个人隐私信息泄漏

移动端忽视对个人信息的保护，导致个人隐私泄漏。从平台层面，由于安全技术漏洞或操作不规范，导致公民个人信息泄漏，降低政府公信力。

缺乏应用监管手段

国家尚未建立专门部门认证应用市场中的移动政务APP，造成山寨政务应用混淆公众视听，破坏政府公信力；公众无法分辨应用发布来源，对信息准确性及个人信息安全构成威胁。

常态化网络安全监测预警

教育部印发的《教育移动互联网应用程序备案管理办法》中提出教育App应当提高事中事后监管能力，各单位应以备案为基础建立监测预警通报机制，及时发现、处置问题隐患和安全事件。

解决方案

电子政务安全解决方案

- **移动安全运营中心**

通过封装底层安全功能组件，并以池化方式部署，能够快速构建常态化、可调度、资源可共享的通用安全能力。

- **公众服务类移动应用、内部办公类移动应用**

目前城市超级App主要是公众服务类移动应用，但也可能存在内部办公类政务移动应用机会。

- **应用安全保障**

应用安全测评、应用合规检测、应用安全防护类产品（Android/iOS/H5加固、密盾）、应用安全监测。

- **数据安全保障**

第三方授权代理查询防护、SDK安全接入管理、移动应用发布渠道管控。

方案优势

- **国办案例的标杆优势：**

各地政务平台需要遵循国办发布的标准，我司为国办的移动安全服务商，将给各省级客户带来信心。

- **服务方案符合客户安全要求：**

通过人工渗透测试发现移动政务App存在的安全问题，通过应用加固、源码加固对移动政务App自身进行安全防护，通过密盾、通信协议保护等安全组件解决数据存储、数据传输安全问题，通过移动威胁感知系统对移动政务App进行运行时监测及监控，覆盖政务App全生命周期安全解决方案。

- **深刻理解客户业务：**

如政务App人脸绕过风险，建立在对客户业务的深刻理解上，快速响应并提供咨询服务，快速提供定制化的安全解决方案。

涉及产品

- **通信认证安全保障：**通信协议保护
- **应用安全保障：**应用测评平台、加固、密盾、应用安全监测、安全SDK、应用合规检测、源码检测、EMM、渠道监测、应用监管平台
- **数据安全保障：**密盾、安全监测产品中的人脸识别绕过功能、人工合规审计服务
- **安全运营服务：**人工渗透测试服务、安全咨询培训服务、人员外包服务、系统平台运营服务