神策数据
SENSORS Data

— 数字化经营系列白皮书 —

神策产品数据安全合规实践

—

Data Security Compliance Practices of Sensors Data Products

前言 Foreword

神策产品数据安全合规的相关说明

承诺未经授权不接触客户数据

神策产品支持私有化部署和 SaaS 部署方式，对于采用私有化部署方式的神策产品的使用者，即系统部署在客户的机房或客户使用的公有云（包括但不限于阿里云、腾讯云、华为云、AWS、Azure 等），相关的安全措施和权限限制均由客户掌握，对于客户机房的数据神策无权获取。对于采用 SaaS 部署方式的神策产品的使用者，神策同样无权接触客户数据，仅出于服务目的对服务资源进行托管。神策对客户服务器的操作仅在获取客户授权后进行，在对相关服务资源进行访问时会使用堡垒机进行严格的权限控制和操作审计，确保操作行为的安全与合规。

神策承诺在提供软件产品和服务过程中，未经客户授权不接触相关数据或报表等形式的统计结果。

提供产品服务仅可被用于合法用途

客户仅可将神策软件产品和服务用于合法用途，客户需要确保其使用神策软件产品和服务的行为符合相关法律法规的规定和监管要求，不侵犯任何第三方的知识产权及其他合法权益，不违反对其有约束力的法律文件的规定。如果客户违反上述约定，神策有权暂停提供产品和服务、并解除本协议。

为了符合《个人信息保护法》关于“收集数据时取得权利所有人授权同意”的要求，客户如使用神策软件产品进行合规数据收集时，需要在《用户隐私说明》文件内，披露第三方 SDK 以及提及神策软件产品。

免责声明

如果客户使用神策软件产品进行数据收集，应当保证数据来源合法合规，或者已经取得相关方和终端用户授权。

客户对终端用户的信息处理应当合法合规，否则神策有权要求客户停止使用神策软件产品进行数据收集和处理，并保留追究责任的权利，且不视为神策违约。

如客户使用神策软件产品对客户指定的第三方进行数据收集和处理，由此行为产生的第三方诉求和相应责任，神策有权要求客户承担或补偿。

目录 Contents

一、当前数据安全态势和背景

1. 法律法规技术标准的颁布

大数据时代的到来，数据已经成为与物质资产和人力资本同样重要的基础生产要素。随着数据价值的凸显和不断挖掘，数据面临的信息安全风险也与日俱增，给个人隐私和国家安全带来了严重的安全隐患。为应对日益严重的安全形势，我国颁布了《数据安全法》和《个人信息保护法》在法律层面为数据安全和个人隐私保护提供法律保障。同时，为了支撑两法落地，网信办、工信部等监管部门出台了《网络数据安全管理条例（征求意见稿）》、《汽车数据安全管理若干规定（试行）》、《工业和信息化领域数据安全管理办法（试行）（征求意见稿）》等行政法规，结合已发布《GB/T 35273-2020 信息安全技术 个人信息安全规范》《JR/T 0171-2020 个人金融信息保护技术规范》等个人信息安全、数据安全标准，共同形成了我国数据安全和个人信息保护的合规监管体系。

2. 日常监管态势的日趋严格

2021 年，App 专项治理仍然是各监管机构数据安全和个人隐私保护治理的重中之重。国家网信办针对人民群众反映强烈的 App 非法获取、超范围收集、过度索权等侵犯个人信息现象，组织对部分 App 的个人信息收集使用情况进行了检测，对存在问题的 App 进行了通报。工信部组织各省通信管理局，持续推进 App 侵害用户权益专项整治行动，加大常态化检查力度，围绕违规收集个人信息、强制索权等隐私合规问题，对未按照要求完成整改的 App 进行通报和下架处理。同时，工信部印发《关于开展信息通信服务感知提升行动的通知》要求相关企业建立已收集个人信息清单和与第三方共享个人信息清单，并在 App 二级菜单中展示，方便用户查询。公安部国家计算机病毒应急处理中心共通报 11 批次移动 App 涉嫌超范围采集个人信息等隐私不合规行为。中国人民银行委托中国互联网金融协会继续开展移动金融 App 的认证备案工作，要求移动金融 App 加强个人金融信息保护，提升安全防护能力。

除此之外，为防范数据安全风险维护国家安全，国家对多家在美上市企业开展网络安全审查，停止其新用户注册。多家银行因金融数据安全问题被银保监会实施行政处罚或通报。企业数据安全合规已经成为业务发展必须面对的重要关卡。

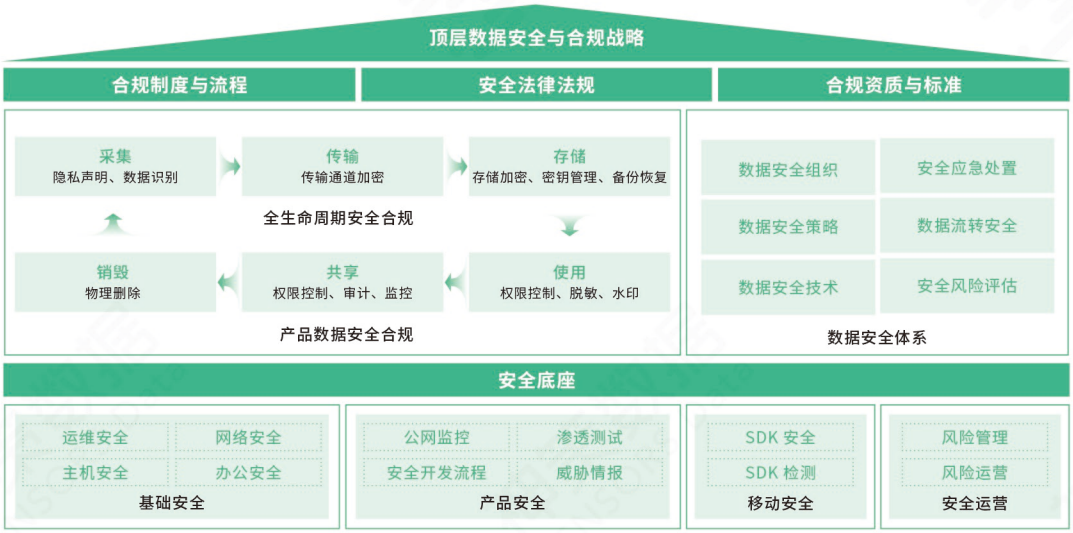
3. 网络安全问题形势严峻

2021 年，全球网络攻击、数据泄漏事件高发，供应链安全成为日益新兴攻击手段，勒索病毒持续激增愈发顽固。2 月，印度航空公司旅客服务系统提供商 SITA 被黑客入侵，约 450 万旅客个人信息泄漏；5 月，加拿大邮政第三方供应商 Commport Communications 遭遇网络攻

击导致 95 万条包裹收件人数据泄漏；名为 DarkSide 的勒索软件攻击了美国主要的燃料管道商佐治亚州殖民地管道公司，严重威胁社会公共服务的安全。12 月，Apache log4j2 远程代码执行漏洞爆发，TellYouThePass、Conti、Mirai、Muhstik 等多个勒索软件和僵尸网络家族利用 Log4Shell 漏洞进行攻击和传播。为了有效应对网络攻击，防止数据泄漏事件发生，需从技术和管理方面提升数据安全能力，保障数据安全。

二、神策的数据安全合规实践

为了应对以上监管和安全态势，神策围绕数据安全的生命周期，从产品的数据安全和合规角度出发，结合数据安全的管理和技术能力，不断提升产品数据安全和合规水平。



1. 数据采集

神策在进行数据采集时严格遵循“合法、正当、必要”的原则，通过隐私政策等方式告知并说明涉及个人信息的权限使用和个人信息处理的目的、方式和范围等规则，在获得最终用户授权同意后开始进行个人信息收集。

神策产品数据采集支持代码埋点、全埋点、可视化全埋点等几种数据采集方式，客户可根据自己的业务需要进行数据采集。

下面从神策数据隐私政策、采集信息情况等方面分别对数据采集的安全及合规场景进行介绍。

场景一：隐私政策及采集信息说明

神策已制定神策数据隐私政策对神策 SDK 在数据采集时的权限申请和信息收集情况进行了详细说明。使用神策产品进行信息收集的客户可依据此内容在其隐私政策中进行信息披露。

1、申请系统权限说明

Android SDK 产品权限说明

神策 Android SDK 需要如下系统权限以保证数据采集的正常展开：

权限	用途	是否必须
INTERNET	允许应用发送统计数据	必须权限，SDK 发送埋点数据需要此权限
ACCESS_NETWORK_STATE	允许应用检测网络状态	必须权限，SDK 会根据网络状态选择是否发送数据
READ_PHONE_STATE	允许应用获取设备 IMEI、MEID	可选权限，采用 App 内推广和采集 $carrier 属性时会用到此权限
ACCESS_WIFI_STATE	允许应用获取 MAC 地址	可选权限，采用 App 内推广时会用到此权限

iOS SDK 产品权限说明

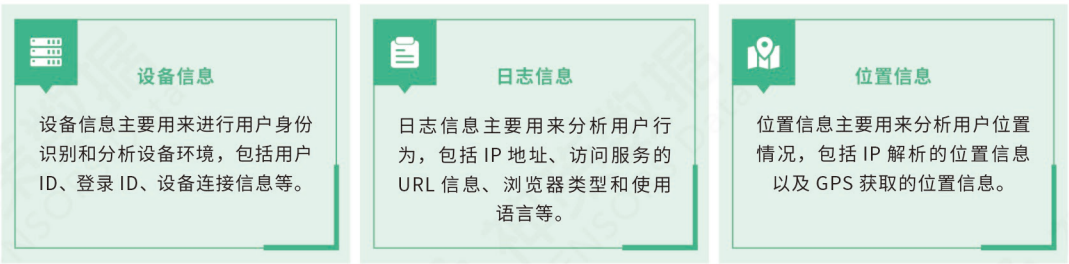
神策 iOS SDK 需要如下系统权限以保证数据采集的正常展开：

权限	用途	是否必须
网络（国服专门）	允许应用发数据	必须权限，SDK 发送埋点数据需要此权限
定位	允许应用获取 GPS 数据	可选权限，SDK 采集 GPS 数据时需要此权限
IDFA	允许应用获取 IDFA	可选权限，采用 App 内推广时会用到此权限

注：1、神策 SDK 不会申请上述权限以外的权限，如果检出名字与神策 SDK 相同的 SDK 有申请上述权限以外的权限，请与神策的工作人员联系，神策数据将会协力排查，避免出现数据安全事故。

2、个人信息采集情况

神策 SDK 具有采集数据的功能，支持自定义设置事件和属性的采集方案。在使用神策全埋点进行数据采集时，用户可根据业务需求开启或者关闭事件采集。全埋点采集涉及个人信息的事件和属性主要包含设备信息、日志信息、位置信息等类型。各类型信息采集情况可参考附录 1。



注意：1、神策 SDK 在采集匿名 ID 的时候，会默认采集 Android ID、IDFA 等设备 ID，如不需要采集以上信息，神策提供了相关接口禁用采集功能。

2、神策 SDK 在采集位置信息时，默认不采集 GPS 位置信息，用户可根据需要进行开启和关闭。

3、神策数据隐私政策可通过访问【神策官网 - 神策分析帮助中心 - 技术指南 - 客户端 SDK- 隐私政策】或直接访问 https://manual.sensorsdata.cn/sa/latest/tech_sdk_client_privacy_policy-22255998.html

场景二：采集行为合规

通过神策 SDK 进行信息采集时，神策 SDK 提供了延迟初始化的方式来满足合规要求，可以在客户明确同意《隐私政策》后，通过初始化 SDK 方式，开始进行数据收集。如果某些控件包含个人敏感信息，神策产品提供 API 可以忽略控件的点击事件，不采集相关信息。

同时在传输至服务端前，神策 SDK 可通过本地加密方式对采集信息中的敏感信息进行保护。

支持延迟初始化和采集缓存加密的版本情况如下：

SDK 名称	延迟初始化支持版本	缓存加密支持版本
Android SDK	v6.0.0 及以上	v6.2.0 及以上
iOS SDK	v1.11.17 及以上	v4.2.0 及以上
Web JS SDK	v1.21.1 及以上	v1.16.10 及以上
小程序 SDK	v1.17.1 及以上	v1.14.9 及以上

1、延迟初始化

以 Android SDK v6.0.0 版本为例，客户在其用户同意《隐私政策》后，初始化 SDK 进行数据收集。

首次在同意隐私条款后调用 SensorsDataAPI.startWithConfigOptions() 初始化 SDK，此后在 Application 的 onCreate() 方法中主线程初始化 SDK。

同时 Android 全埋点提供了 API 可以忽略控件的点击事件采集，如：

```
SensorsDataAPI.shareInstance().ignoreView(View view);
```

2、采集缓存加密

神策产品通过 SDK 进行信息采集时，在传输至服务端前通过本地加密方式对采集信息中的敏感信息进行保护。以 Web JS SDK 为例：

Web JS SDK 保存的 cookie 中包含部分用户信息及 register 设置的属性信息，为保证该类信息在传输至服务端前的安全，神策提供 cookie 加密功能保证数据安全。

```
<script charset="UTF-8">
    var sensors = window["sensorsDataAnalytic201505"];
    // 初始化 SDK
    sensors.init({
      server_url: " 数据接收地址 ",
      // 开启 cookie 加密配置，默认 false
      encrypt_cookie: true
    });
    sensors.quick("autoTrack");
  </script>
```

注意：客户一旦使用加密功能，那么必须保证所有页面的 SDK 必须是最新版；否则如果某些页面使用了加密 cookie 的功能，那么 cookie 就是加密的，一旦个别页面使用的是老版本 SDK ，没有解密功能，都会导致无法解析 cookie ，从而造成产生新用户，用户无法统一。

SDK 延迟初始化及本地加密配置方式请访问神策官网并点击【神策分析帮助中心 - 技术指南 - 客户端 SDK- 合规说明 - 数据收集安全说明】或者直接访问以下链接获取：https://manual.sensorsdata.cn/sa/latest/tech_sdk_client_compliance-60129330.html#id-.合规说明 v2.3- 数据收集安全说明

2. 数据传输

神策产品在数据采集完成后，在进行采集数据传输时，可采用链路加密或者数据加密的方式进行数据传输，保障传输数据的安全。

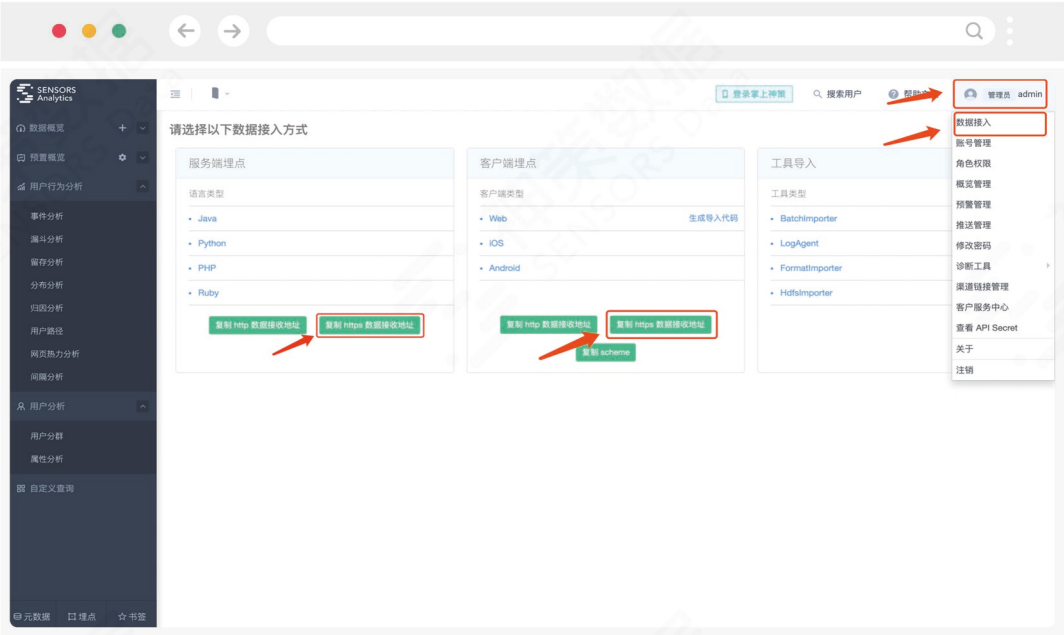
下面分别从链路加密和数据加密两个方面对数据传输的安全场景进行介绍。

场景一：传输链路加密

神策产品通过 HTTPS 技术建立不同安全域间的加密传输链路，支持配置 HTTPS 数据接入，配置参考文档链接：https://manual.sensorsdata.cn/sa/latest/page-7539390.html

1、SaaS 部署版本 HTTPS 接入

以神策分析 SaaS 部署版本为例，默认已经配置了 HTTPS 数据接入，可直接获取对应的 HTTPS 数据接入地址使用。使用管理员账户在神策分析页面获取 HTTPS 数据接入地址：



2、私有化部署版本 HTTPS 接入

神策产品私有化部署版本支持在云厂商的负载均衡或硬件负载上配置 HTTPS，也支持独立部署的其他开源应用上配置 HTTPS，客户可根据自己业务的实际情况开启 HTTPS。

在云厂商的负载均衡或者硬件负载设备启用 HTTPS

常见负载均衡设备均提供 HTTPS 接入功能，可根据实际情况选择不同云厂商的 LB 或者硬件负载设备来开启 HTTPS；

使用 HTTPS 加密传输需要提供 SSL 证书，神策不提供任何 SSL 证书。该证书可以通过多种渠道获取，若使用自签证书请确保客户端信任该证书；

使用 HTTPS 请关注证书的过期时间，若证书过期可能会导致数据无法发送成功。

如果是第一次使用云厂商的负载均衡，建议查看各厂商负载均衡配置官方文档：

阿里云：

https://help.aliyun.com/product/27537.html?spm=a2c4g.750001.list.58.58ec7b13d6ngZn

腾讯云：

https://cloud.tencent.com/document/product/214

AWS 云：

https://docs.aws.amazon.com/zh_cn/elasticloadbalancing/?id=docs_gateway

Ucloud：

https://docs.ucloud.cn/network/ulb/overview

华为云：

https://support.huaweicloud.com/elb/index.html

在独立部署的其他开源应用上配置 HTTPS

从机器成本和人力成本考虑，如非必要，神策不建议采用此方案。

若需在独立部署的其他开源应用上配置 HTTPS，需要额外一台或多台（确保高可用）机器来部署开源负载均衡应用，不能部署在神策的机器上。同时，请自行规划负载均衡应用所在机器的配置、高可用和监控方案。如需使用此种方式配置 HTTPS，请联系神策技术支持。

3、HTTPS 配置验证

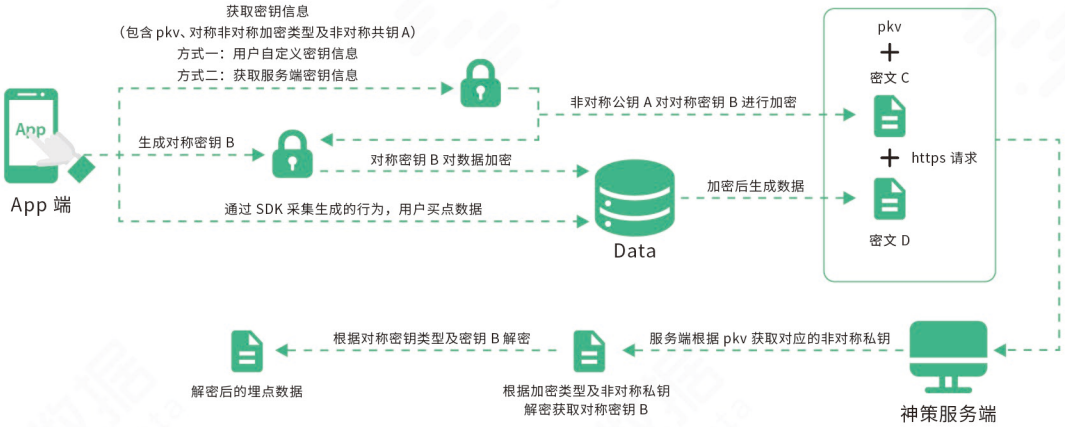
在完成 SaaS 部署版或者私有部署版 HTTPS 配置后，需对神策后台配置进行更新，神策后台需要知道对应的 HTTPS 地址，所以还需要在神策服务中配置 HTTPS URL，否则会影响部分功能的使用，包括：埋点代码生成功能、渠道管理功能。

场景二：传输数据加密

针对部分敏感级别比较高的埋点数据，除采用 HTTPS 方式实施链路加密外，神策支持对埋点数据进行加密，并以密文的形式对数据进行传输。

SDK 名称	数据加密支持版本	是否支持国密算法
Android SDK	v4.2.0 及以上	是
iOS SDK	v2.1.0 及以上	是
Web JS SDK	Web JS SDK v1.19.9 及以上、Edge v0.3.0 及以上、SDF v2.3 及以上	否
小程序 SDK	小程序 SDK v1.14.27 及以上版本、Edge v0.3.0 及以上版本、SDF v2.3 及以上版本	否

以神策 Android SDK 和 iOS SDK 为例，数据加密支持使用 AES+RSA、SM2+SM4 等加密算法，同时支持使用自定义加密插件方式进行数据加密算法管理，实现数据加密传输。加解密过程如下：



SDK 加密过程示例（AES+RSA）：

使用 AES 对采集的明文数据集进行加密

使用 RSA 加密对 AES 的秘钥进行加密

把密文数据和 AES 秘钥密文发送给服务端。

服务端拿到数据解密过程示例：

使用 RSA 的私钥对 AES 秘钥密文解密，得到 AES 秘钥

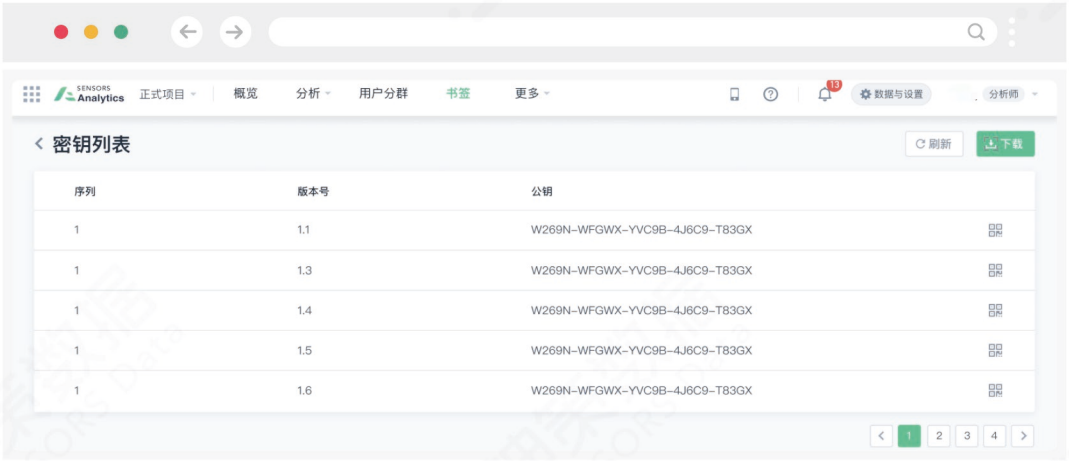
使用 AES 秘钥对密文数据解密，得到明文数据

对数据进行校验入库。

在完成 SDK 端开启加密配置后，需要对加密密钥进行验证，以神策分析平台为例：

在神策分析平台中，进入密钥管理功能，进入路径：「更多」→「基本设置」→「数据接入」→「密钥管理」

点击「密钥管理」按钮进入密钥管理页面



其余版本 SDK 传输加密配置方式请访问神策官网并点击【神策分析帮助中心 - 技术指南 - 客户端 SDK】获取或直接访问以下链接：

Android SDK：

https://manual.sensorsdata.cn/sa/latest/tech_sdk_client_android_super-7538650.html#id-.SDKAPI(Android)v1.13- 埋点数据的加密功能

iOS SDK：

https://manual.sensorsdata.cn/sa/latest/tech_sdk_client_ios_super-22253311.html#id-.SDKAPI(iOS)v1.13- 埋点数据的加密功能

Web JS SDK：

https://manual.sensorsdata.cn/sa/latest/tech_sdk_client_web_high-42795073.html#id-.SDKAPI(Web)v2.3- 埋点数据的加密功能

小程序 SDK：

https://manual.sensorsdata.cn/sa/latest/page-40206469.html#id-.SDKAPI(小 程 序) v2.3- 埋点数据的加密功能

3. 数据存储

神策产品在数据存储阶段充分考虑数据防泄漏的问题，通过对入库数据加密，可以有效防止因内外部恶意行为导致的数据泄漏风险。

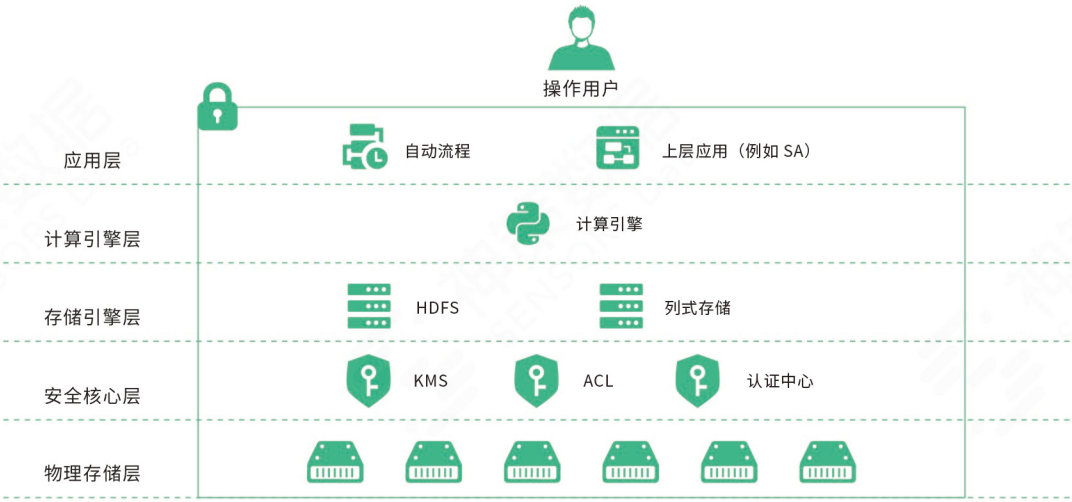
神策产品支持的加密方式包括应用层加密和透明加密方式：

透明加密：透明加密产品一般通过拦截数据库数据文件的读写操作完成加解密，即，数据文件落盘时自动加密，数据文件被读取时自动解密。这种加密方式无须修改应用层代码，且通过技术手段可以实现密文索引，应用较广。

应用层加密：写入时，应用层代码执行加密操作，并将加密后的数据存到数据库中；读取时，应用层代码从数据库读取密文，并将密文进行解密。

场景一：存储加密

神策产品通过统一的密钥管理手段，实现存储系统和其上的计算引擎的加密和解密。整个加密流程中，通过 ACL 管理密钥和数仓内各层应用的访问授权，通过认证中心实现神策各个服务之间的身份验证。系统关系如下：



除整体的存储透明加密外，神策产品还针对登录用户手机号、登录密码等用户个人敏感信息，通过应用加密方式进行数据加密存储。

4. 数据共享使用

数据作为一种重要的基础生产要素，充分的分析和挖掘才能释放数据更大的内在价值，但是

数据泄漏的风险也与日俱增。不恰当的数据使用、频繁的数据共享流动等都会增加数据泄漏的风险。因此在数据共享使用过程中应采取有效的措施防范数据泄漏风险，保障数据安全。

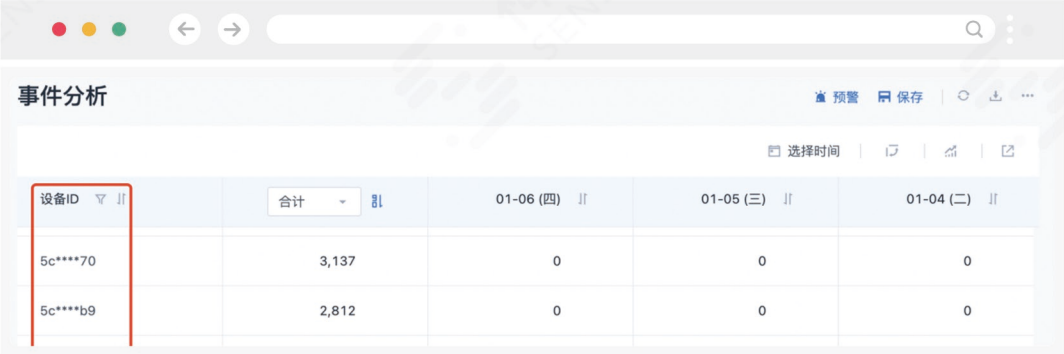
神策产品遵循最小化原则，并充分考虑数据的可用性和安全性之间的平衡，提供数据脱敏展示等方式帮助客户降低数据泄漏的风险。同时，在发生数据泄漏风险时通过数据水印等手段进行有效的事件溯源。

场景一：数据脱敏展示

在进行数据使用时，涉及通过界面展示个人信息的场景，神策产品支持用户通过自定义方式进行数据脱敏展示，用户可以选择对相关用户属性和事件属性进行脱敏展示，设置脱敏展示界面如下：

脱敏展示规则参照相关行业最佳实践，同时结合神策产品的数据分析、展示的需求制定。例如手机号码 18999999988 和 18999998888 脱敏后将被显示为 18****88_1 和 18****88_2。

脱敏后的界面展示示例：



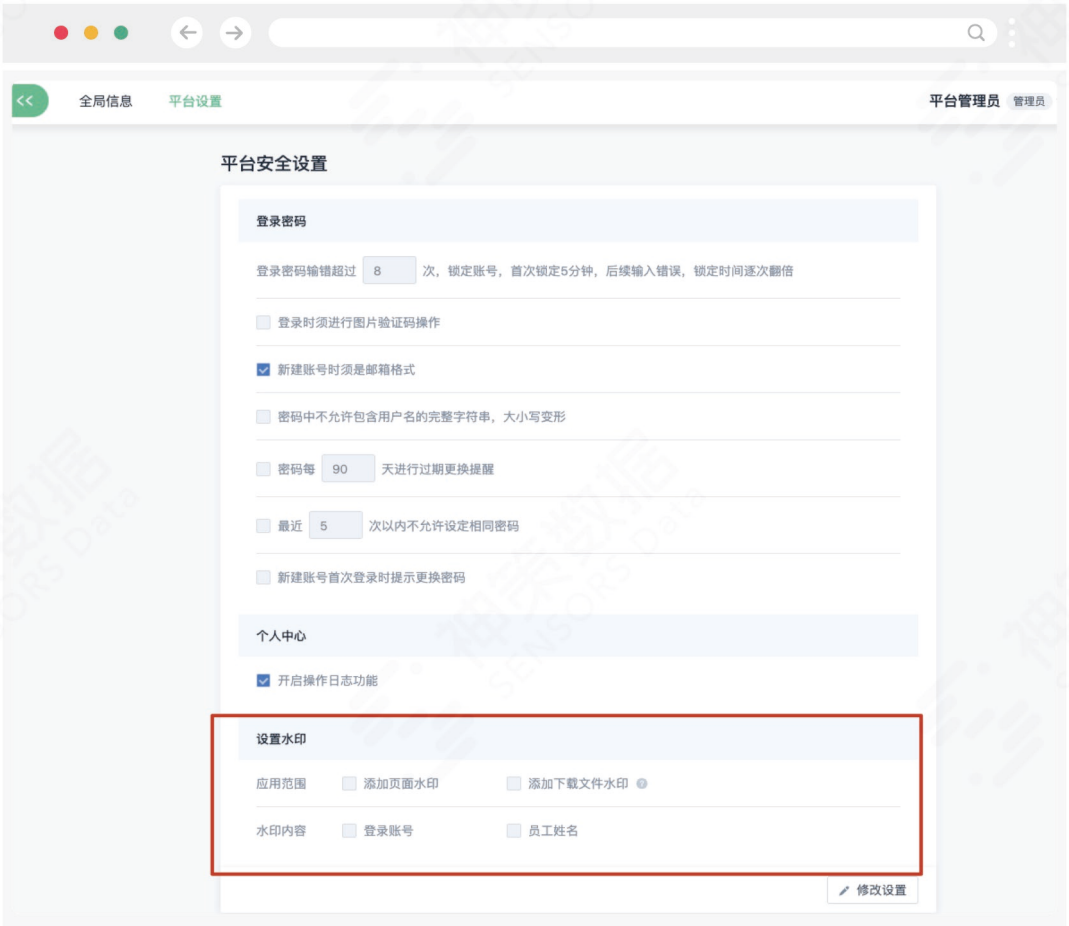
注意：用户属性和事件属性选择脱敏展示后将不再支持使用脱敏属性标签进行筛选，如果需要对该属性进行筛选可以另外创建不脱敏显示的角色和成员。

场景二：数据产品水印

水印是一种数字保护的手段，在图像上添加水印即能证明本人的版权，还能对版权的保护做出贡献。在神策的理念中，客户的数据安全一直是重中之重。因此我们希望借助于水印来保护客户的数据安全以及在发生数据泄密时追根溯源。

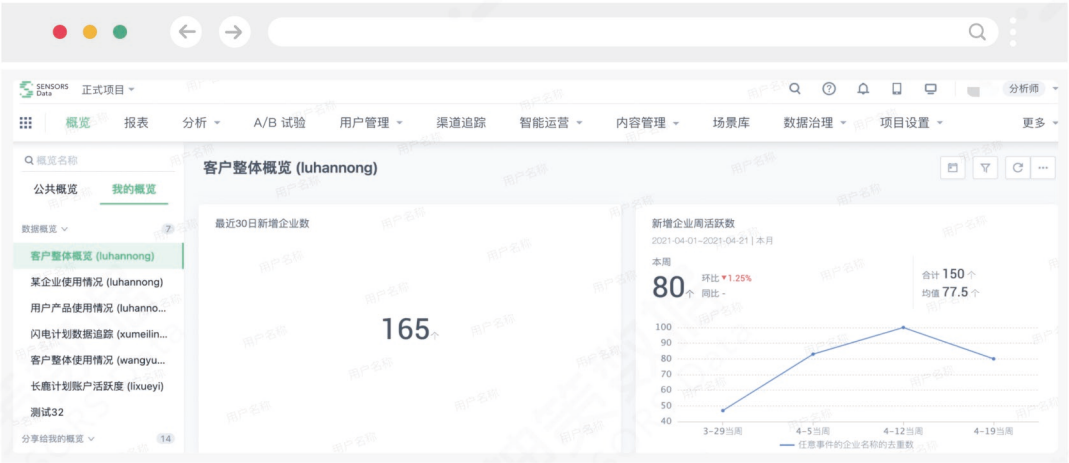
神策产品通过平台安全设置模块支持自定义设置水印范围和水印内容，管理员用户可通过设置水印，降低通过截屏、录屏等方式引起的数据泄漏情况的发生。

水印设置页面：

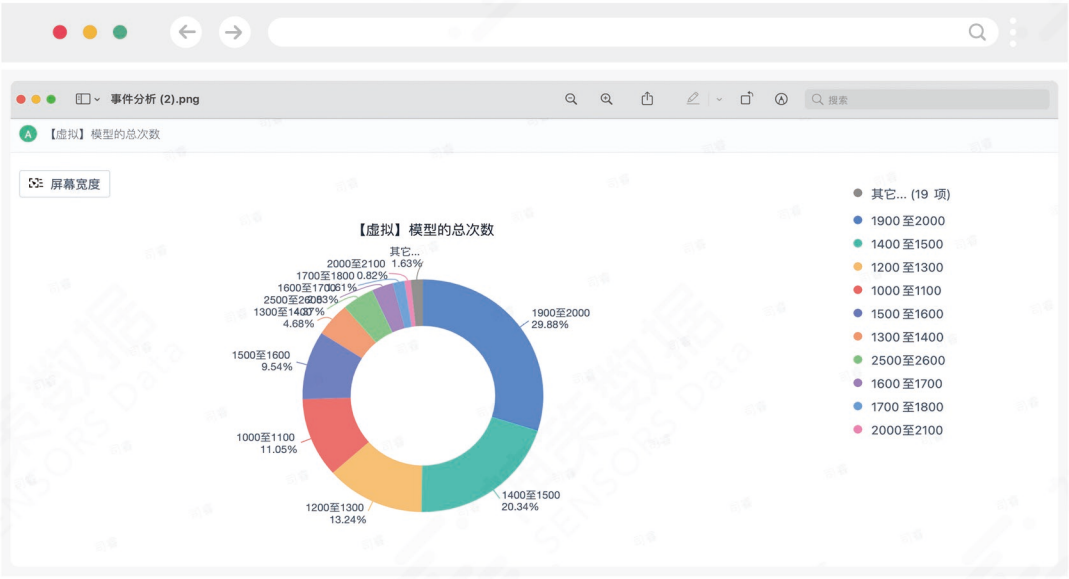


设置好水印之后，可以在访问页面和下载的文件时查看到水印情况：

页面水印示例：



下载文件水印示例：

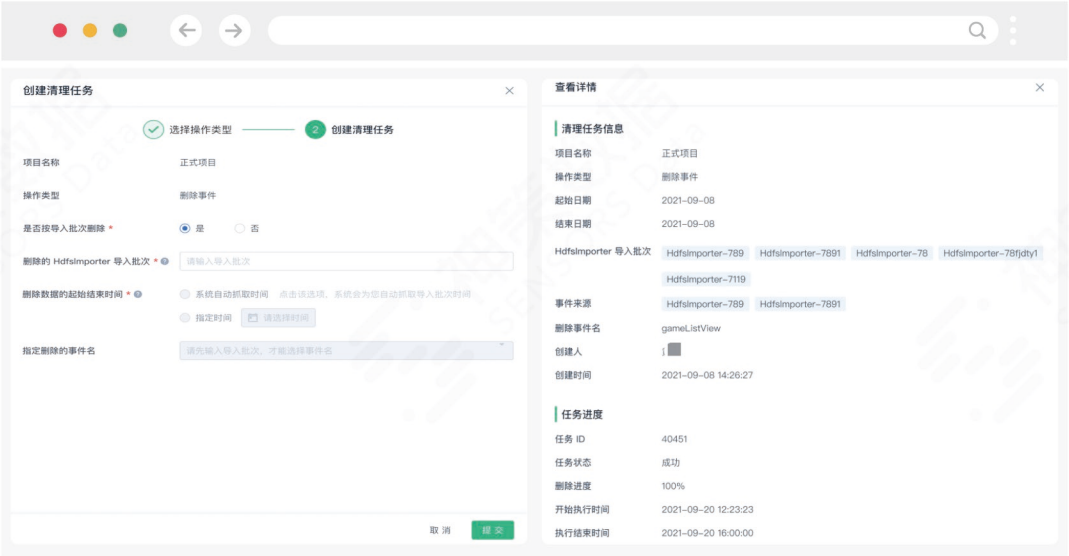


5. 数据删除和销毁

神策产品严格按照相关法律法规的要求，为用户提供选择退出机制，当神策的用户或者个人信息主体不希望使用神策提供的数据产品和数据服务时，可以停止神策 SDK 的数据采集功能，并使用神策产品提供的数据清理工具进行数据删除，数据删除支持批量删除事件数据和基于用户 ID 删除用户数据两个功能。

场景一：批量删除事件数据

神策产品提供界面化的批量事件数据删除功能，用户可以按照导入批次号、日期、事件名等进行事件删除。



场景二：删除指定用户数据

神策提供界面化的用户数据删除功能，支持通过用户 id 批量删除 event 和 users 表中的数据和用户关系。

注意：1、基于产品性能考虑，删除工具默认删除 180 天内的事件数据，如果需要删除全量或更长时间的事件数据，可通过修改默认删除数据时间方式进行；

2、为降低频繁删除数据对产品性能的影响，默认 15 个工作日删除一次。

6. 访问控制与行为审计

神策产品提供基于 4A 的统一的用户登录功能，可以实现基于角色的访问控制功能。4A 功能如下：

1）Account（账号）：神策产品为每个用户创建唯一的用户账号，并对用户身份进行鉴别，确保数据访问控制和安全审计可以追溯到个人账号。同时，采用基于角色的用户分组管理，将系统管理角色、系统数据建设角色和数据查看角色进行区分。

2）Authentication（鉴别）：神策产品的数据访问依托于统一的身份鉴别机制，通过统一的登录身份认证技术实现用户身份鉴别管理。

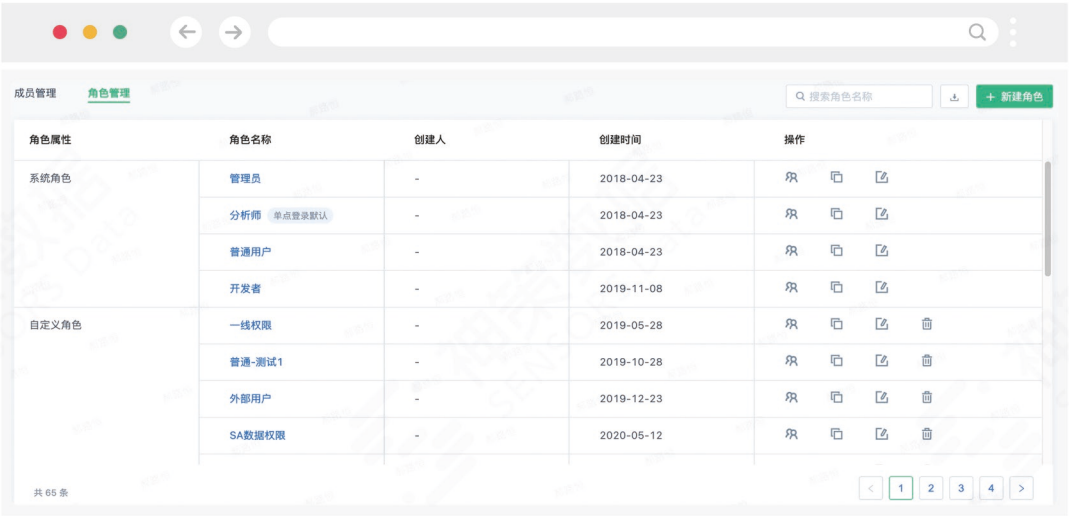
3）Authorization（授权）：神策产品根据数据访问主体的角色不同，实现对各类数据严格的访问授权。

4）Audit（审计）：神策产品通过日志和审计功能，实现对系统中角色管理、成员管理、用户登录、数据获取 / 访问 / 修改等行为的完整日志记录。基于系统审计日志，可以实现事中的安全监控，以及事后的行为溯源和取证分析。

场景一：角色管理和访问控制

有效的身份认证与访问控制是确保客户数据不被非授权访问的关键。神策为客户预制了多种

不同权限的角色，同时客户也可以根据需要创建更多的角色。根据角色权限的不同，数据访问将会被严格控制。



神策还为客户提供了基于 API 的数据访问方式，每一个在神策中存在的账号，均有其对应的唯一 Token，通过对访问请求中 Token 的认证，可以严格控制数据访问权限。

神策同时还提供了通过 OAuth2.0 协议，与客户自有的账号体系进行集成对接，所有的访问权限均可由客户自行控制。

场景二：日志留存和审计

神策产品已实现统一的日志留存和审计功能，可以对用户登录登出、敏感操作等信息进行日志留存和审计。操作日志默认留存的时间为 6 个月，企业用户也可以根据业务实际，调整日志留存的时间。

审计情况如下：

三、神策安全相关资质认证

1. 信息安全管理体系认证（ISO 27001）

ISO 27001 是有关信息安全管理的国际标准，该标准可用于组织信息安全管理体系的建立和实施，旨在通过明确的管理控制实现信息安全。ISO 27001 通过采用 PDCA 的过程方法，参考一系列的最佳实践，基于风险评估的风险管理理念，持续改进组织的信息安全管理水平。

神策数据已于 2020 年 9 月通过 ISO 27001 的认证审核：

ZJQC

中经认证

注册号：04420IS0252R1M

信息安全管理体系
认证证书

兹证明

神策网络科技（北京）有限公司

统一社会信用代码：91110108339829205 7

注册地址：北京市海淀区知春路 27 号 11 层 1101-1108 室

审核地址：北京市海淀区知春路 27 号量子芯座 1101-1112、1501-1512 室

信息安全管理体系符合

GB/T22080-2016/ISO/IEC27001:2013 标准

该体系覆盖范围

与应用软件开发及其运维服务相关的信息安全管理活动

适用性声明（版本：A/2，发布日期：2021 年 07 月 17 日）

（未纳入认证范围的多场所不得使用认证证书和认证标志）

颁证日期：2020 年 09 月 11 日　有效期至：2023 年 09 月 11 日　换证日期：2021 年 09 月 07 日

北京中经科环质量认证有限公司　总经理：

1. 本证书有效性查询可扫描左侧二维码
2. 同时可登陆 www.zjqc.com 查询
3. 也可登陆国家认证认可监督管理委员会官方网站 www.cnca.gov.cn 查询
4. 获证组织必须定期接受监督审核并经审核合格此证书方继续有效

公众号　证书查询

日　期：2021 年 09 月 07 日

中国认可
国际互认
管理体系
MANAGEMENT SYSTEM
CNAS C044-M

地址：北京市西城区月坛北小街4号5号楼1429

2. 隐私信息管理体系认证（ISO 27701）

ISO 27701 标准将隐私保护的原则、理念和方法，融入到信息安全保护体系中，以ISO27001和ISO 27002扩展的形式为建立、实施、维护和持续改进隐私信息管理体系提供了指南，并且对 PII 控制者和 PII 处理者进行了较为详细且落地性强的规定，给企业在隐私保护和信息安全方面给出了指导建议。

神策数据已于 2021 年 12 月通过 ISO 27701 的认证审核：

中经认证

注册号：04421PIMS0003R0M

隐私信息
管理体系认证证书

兹证明

神策网络科技（北京）有限公司

统一社会信用代码：911101083398292057

注册地址：北京市海淀区知春路 27 号 11 层 1101-1108 室

审核地址：北京市海淀区知春路 27 号量子芯座 1101-1112、1501-1512 室

隐私信息管理体系符合

ISO/IEC 27701:2019 标准

该体系覆盖范围

与神策软件应用体验服务相关的隐私信息保护管理活动

适用性声明（版本：B/1）

（组织已按照 ISO/IEC 27001:2013 标准建立了信息安全管理体系）

（未纳入认证范围的多场所不得使用认证证书和认证标志）

颁证日期：2021 年 12 月 02 日　　有效期至：2024 年 12 月 01 日

北京中经科环质量认证有限公司　　总经理：

日　期：2021 年 12 月 02 日

公众号　证书查询

1. 本证书有效性查询可扫描左侧二维码
2. 同时可登陆 www.zjqc.com 查询
3. 也可登陆国家认证认可监督管理委员会官方网站 www.cnca.gov.cn 查询
4. 获证组织必须定期接受监督审核并经审核合格此证书方继续有效

地址：北京市西城区月坛北小街4号5号楼1429

3. 质量体系认证（ISO 9001）

ISO 9001 是衡量企业质量管理活动状况的一项国际标准，通过以过程为基础的质量管理体系机构模式，围绕管理职责、资源管理、过程管理、测量分析与改进四个重要组成部分，结合 PDCA 循环和基于风险的思维，帮助企业在创建产品或服务过程中提高整体绩效，推动可持续发展。

神策数据已于 2020 年 9 月通过 ISO 9001 的认证审核：

ZJQC

中经认证

注册号：04420Q11564R1M

质量管理体系认证证书

兹证明

神策网络科技（北京）有限公司

统一社会信用代码：911101083398292057

注册地址：北京市海淀区知春路 27 号 11 层 1101-1108 室

审核地址：北京市海淀区知春路 27 号 11 层 1101-1108 室、1501-1512 室

质量管理体系符合

GB/T 19001-2016/ISO 9001:2015 标准

该体系覆盖范围

应用软件开发及其服务

（未纳入认证范围的多场所不得使用认证证书和认证标志）

颁证日期：2020 年 09 月 11 日　　有效期至：2023 年 09 月 11 日

北京中经科环质量认证有限公司　　总经理：

1. 本证书有效性查询可扫描左侧二维码
2. 同时可登陆 www.zjqc.com 查询
3. 也可登陆国家认证认可监督管理委员会官方网站 www.cnca.gov.cn 查询
4. 获证组织必须定期接受监督审核并经审核合格此证书方继续有效

公众号　　证书查询

日　期：2020 年 09 月 11 日

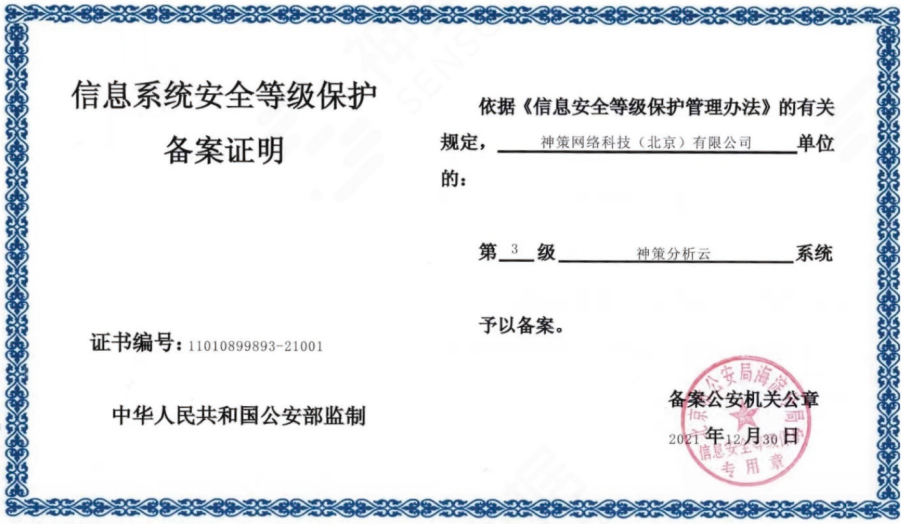
中国认可
国际互认
管理体系
MANAGEMENT SYSTEM
CNAS C044-M

地址：北京市西城区月坛北小街4号5号楼1429

4. 等级保护

根据《中华人民共和国网络安全法》相关要求，国家实行网络安全等级保护制度，网络运营者应当按照网络安全等级保护要求，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄漏或者被窃取。

神策数据分析云和营销云两个 SaaS 部署的系统已于 2022 年 1 月通过等级保护三级备案，按照《GB/T22239-2019 信息安全技术 网络安全等级保护基本要求》内容落实等级保护防护技术要求和管理要求。



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，神策网络科技（北京）有限公司单位的：

第 3 级 神策分析云 系统

予以备案。

证书编号：11010899893-21001

中华人民共和国公安部监制

备案公安机关公章

2021 年 12 月 30 日

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，神策网络科技（北京）有限公司单位的：

第 3 级 神策营销云 系统

予以备案。

证书编号：11010899893-21002

中华人民共和国公安部监制

备案公安机关公章

2021 年 12 月 30 日

5.SDK 安全专项评测

SDK 安全专项测评是由中国信息通信研究院大数据应用与安全创新实验室发起的“SDK 安全专项行动”，通过对 Android SDK 的基础安全、数据安全存储、数据安全交互、重要组件安全、代码及资源文件安全等进行评测，综合评价 SDK 的安全水平。

神策数据 2021 年 10 月通过 SDK 安全专项行动的评测并获颁证书：


证书编号：AQS-SJ-2021-045
报告编号：2021SJAQ045

CAICT
中国信通院

大数据应用与安全创新实验室
评测证书

神策网络科技（北京）有限公司

经大数据应用与安全创新实验室评测，神策网络科技（北京）有限公司 的 神策数据 Android SDK（版本号：5.4.2）通过 SDK 安全专项评测，特发此证。

评测项目：基础安全、数据存储安全、数据交互安全、重要组件安全、代码及资源文件安全

声明：本证书真实性可通过大数据应用与安全创新实验室公众号查询，评测结果详情可见对应编号的检验报告。本证书仅对检验报告（2021SJAQ045）检测项结果负责，若该产品发生修改或版本升级，需另行评测。

证书查询二维码

中国信息通信研究院
China Academy of Information and Communications Technology
二〇二一年十月

6.CMMI3

CMMI 全称是 Capability Maturity Model Ingegration，即软件能力成熟度模型集成，其目的是帮助软件企业对软件工程进行管理和改进，增强开发与改进能力，开发出高质量软件。CMMI 为改进组织的各种过程提供了一个自动的可扩展的框架，从而能从整体上改进组织的质量和效率。CMMI 主要关注点是成本效益、明确重点、过程集中和灵活性几方面。CMMI3 是其中的一个等级 - 定义级。在该级别上，企业不仅能对项目实施一整套的管理措施，保障项目完成，而且可以根据自身情况和标准化流程，将整套体系制度化。

神策数据 2019 年 8 月通过 CMMI3 的认证审核：


CMMI Institute Partner

SG CMC

Completed an official Standard CMMI® Appraisal Method for Process Improvement (SCAMPI) appraisal (ID: 4142) on 9 August 2019 in accordance with the CMMI Institute's CMMI® Appraisal Requirements and judged

神策数据 SENSORS Data

Sensors Data Co., Ltd.

神策网络科技(北京)有限公司

P.R. of China

to be at CMMI Institute Process Maturity Level 3 as defined by the CMMI® for Development V1.3

Kwangsik Shin, Appraisal Team Leader

CMMI Institute Authorized Lead Appraiser (ID No. 0300323-01)

℠ Standard CMMI Appraisal Method for Process Improvement and SCAMPI are service marks of CMMI Institute.

® CMMI is registered in the U.S. Patent and Trademark Office by CMMI Institute.

四、神策行业资格

神策数据积极践行数据合规，并参与行业内众多合规活动。

神策数据参与的合规组织：

全国信息技术标准化委员会大数据标准化工作组

全国信息安全标准化委员会大数据标准特别工作组

中国通信标准化协会大数据工作组

中国大数据产业生态联盟

中国电子工业标准化技术协会信息技术应用创新工作委员会

北京信息化协会信息技术应用创新工作委员会

中国网络安全产业联盟

中国电子商会数据资源专家委员会

神策数据参与的标准制定：

参与全国信息安全标准化技术委员会《信息安全技术 移动互联网应用程序（App）软件开发工具包（SDK）安全要求》国家标准编写。

参与中国通信标准协会大数据技术标准推进委员会《大数据 用户行为分析 第 1 部分 技术要求》（DSC 19-2018）《大数据 用户行为分析 第 2 部分：测试方法》（DSC 20-2018）编写。

神策数据参与的行业内合规活动：

2020 年（第六届）中国互联网法治大会成立移动互联网用户信息安全保护相关工作组织，包括神策数据、阿里巴巴、字节跳动、华为、百度、小米在内的 46 家企 / 事业单位、研究机构等获准加入。

2020 年 11 月 27 日，工业和信息化部组织的全国 App 个人信息保护监管会发布《App 用户权益保护测评规范》10 项标准及《App 收集使用个人信息最小必要评估规范》8 项标准， 作为互联网协会成员单位，神策数据创始人 & CEO 桑文锋宣读《App 个人信息保护公开承诺书》。

2021 年，神策入选中国信通院开源供应商目录。

2021 年，神策入选个人信息保护合规审计推进小组名单。

五、结束语

神策将一直践行合规发展理念，致力于打造开放、安全的用户行为分析系统，竭诚为客户提供稳定、可靠、安全、合规、透明、公开、对等的用户行为分析系统基础服务。在提供服务过程中，神策始终捍卫客户的数据安全，帮助客户保护其数据的安全，提升客户数据的可用性、保密性和完整性。

附录 1： 神策 SDK 采集个人信息情况说明

设备信息：

Personal Data 处理的个人信息	Property Display name 属性显示名	Purpose of Processing 处理目的	Remark 备注
匿名用户 ID	国际移动设备身份码 IMEI	用户身份识别	支持关闭采集
	iOS 广告标识符 IDFA	用户身份识别	支持关闭采集
	iOS 广告标识符 IDFV	用户身份识别	
	iOS UUID	用户身份识别	
	Android 设备 Android ID	用户身份识别	支持关闭采集
	Android 设备 OAID	用户身份识别	支持关闭采集
	Web 端 cookie_id	用户身份识别	
	小程序 open_id	用户身份识别	
	小程序 union_id	用户身份识别	
登录 ID	用户 ID	用户身份识别	自定义代码传入
设备连接信息	运营商	分析设备环境	
	设备品牌	分析设备环境	
	设备制造商	分析设备环境	
	设备型号	分析设备环境	
	网络类型	分析设备环境	
	操作系统	分析设备环境	
	操作系统版本	分析设备环境	
	UserAgent	分析设备环境	默认不采集
	是否 WIFI	分析设备环境	

日志信息：

Personal Data 处理的个人信息	Property Display name 属性显示名	Purpose of Processing 处理目的	Remark 备注
IP 地址	IP	分析行为日志	Nginx 解析
	IP 运营商	分析行为日志	根据 IP 解析
所访问服务的 URL 相关信息	页面标题	分析行为日志	
	页面地址	分析行为日志	默认不采集
	页面地址域名	分析行为日志	
	页面地址路径	分析行为日志	
	页面地址参数	分析行为日志	
	启动场景	分析行为日志	
	页面名称	分析行为日志	
	前向地址	分析行为日志	
	前向域名	分析行为日志	
	前向页面标题	分析行为日志	
最近所访问服务的 URL 相关信息	最近一次落地页	分析行为日志	
	最近一次站外前向地址	分析行为日志	
	最近一次启动场景	分析行为日志	
	最近一次搜索引擎关键词	分析行为日志	
	最近一次分享深度	分析行为日志	
	最近一次分享者	分析行为日志	
	最近一次分享途径	分析行为日志	
浏览器类型和使用的语言	浏览器	分析行为日志	根据 UA 解析
	用户浏览器语言	分析行为日志	根据 UA 解析
	浏览器版本	分析行为日志	根据 UA 解析
与通讯软件通讯的信息	事件触发的时间	分析行为日志	
	时区偏移量	分析行为日志	
	事件时长	分析行为日志	

位置信息：

Personal Data 处理的个人信息	Property Display name 属性显示名	Purpose of Processing 处理目的	Remark 备注
IP 地址相关位置	国家	分析位置信息	根据 IP 地址解析
	省份	分析位置信息	根据 IP 地址解析
	城市	分析位置信息	根据 IP 地址解析
GPS	地理位置坐标系	分析位置信息	默认不采集
	纬度	分析位置信息	默认不采集
	经度	分析位置信息	默认不采集

唯一应用程序编号：

Personal Data 处理的个人信息	Property Display name 属性显示名	Purpose of Processing 处理目的	Remark 备注
唯一应用程序编号、应用名称	应用唯一标识	分析应用信息	
	应用名称	分析应用信息	
	应用版本	分析应用信息	

其他非个人信息数据采集情况可参照：

https://manual.sensorsdata.cn/sa/latest/tech_sdk_client_compliance-60129330.html

关于神策数据

神策数据（Sensors Data）是国内专业的大数据分析和营销科技服务提供商，为企业提供神策营销云、神策分析云、神策数据根基平台三大产品方案，通过全渠道的数据采集与全域用户 ID 打通，全场景多维度数据分析，全通道的精准用户触达，帮助企业实现数字化经营。

神策数据立足大数据及用户行为分析的技术与实践前沿，提出基于数据流的企业运营框架——SDAF，即 Sense（感知）、Decision（决策）、Action（行动）、Feedback（反馈）的数据闭环，并致力为客户打造基于 SDAF 运营框架的数据闭环。业务现已覆盖以互联网、品牌零售、金融、融合媒体、企业服务、高科技、汽车、互联网 + 等为代表的 30 多个主要行业，并可支持企业多个职能部门，目前已服务付费客户 2000 余家。公司总部在北京，并在上海、深圳、合肥、武汉、成都、中国台北等地均拥有本地化的服务团队，覆盖全国及东南亚市场。同时，公司拥有专业的服务团队，为客户提供与营销和大数据相关的咨询、解决方案和专业服务。

关于神策研究院

神策研究院，旨在围绕数字化经营相关领域，提供更具行业深度的洞察、领先的行业实践，秉持开放、创新、前瞻的研究视野，利用数据驱动的科学方法推进企业数字化转型。

声明

作者：
张　娜　　神策数据安全总监
苏　硕　　神策数据安全工程师

美术编辑：
曹　阳　　神策数据高级设计师

神策数据
SENSORS Data

联系我们
邮箱：contact@sensorsdata.cn
电话：400 650 9827
网址：www.sensorsdata.cn

关注神策数据　　关注神策学堂　　扫码咨询顾问