CAICT 中国信通院

应用程序接口（API）数据安全研究报告

（2020 年）

中国信息通信研究院安全研究所

2020 年 7 月

版权声明

前　言

伴随着云计算、大数据、人工智能等技术的蓬勃发展，移动互联网、物联网产业加速创新，移动设备持有量不断增加，Web 应用、移动应用已融入生产生活的各个领域。这一过程中，应用程序接口（Application Programming Interface，API）作为数据传输流转的重要通道发挥着举足轻重的作用。API 技术不仅帮助企业建立与客户沟通的桥梁，还承担着不同复杂系统环境、组织机构之间的数据交互、传输的重任。然而，在 API 技术带来上述积极作用的同时，与其相关的数据安全问题也日益凸显。

近年来，国内外曝出多起与 API 相关的数据安全事件，严重损害了相关企业、用户的合法权益。我国多个行业已出台相关规范性文件，覆盖通信、金融、交通等诸多领域，对 API 安全提出了一定要求，对其技术部署、安全管理等进行规范。然而当前已研制标准主要针对特定 API 类型、应用场景提出要求，尚未全面覆盖 API 数据安全，相关标准规范体系有待完善。

本报告围绕近年来 API 安全态势，分析梳理了 API 技术面临的内、外部安全风险，针对事前、事中、事后不同阶段的安全需求差异，从 API 安全管理、防护手段、风险管控等多角度为企业实现高效、灵活的 API 安全实践提出了针对性建议。

技术支持：

全知科技（杭州）有限责任公司

联系人：

王丹辉　中国信息通信研究院

电子邮件：wangdanhui@caict.ac.cn

解伯延　中国信息通信研究院

电子邮件：xieboyan@caict.ac.cn

朱通　全知科技（杭州）有限责任公司

费媛　全知科技（杭州）有限责任公司

目 录

表 目 录

一、API 的基本情况

伴随着云计算、移动互联网、物联网的蓬勃发展，越来越多的开发平台和第三方服务快速涌现，应用系统与功能模块复杂性不断提升，应用开发深度依赖于应用程序接口（Application Programming Interface，API）之间的相互调用。近年来移动应用深入普及，促使社会生产、生活活动从线下转移到了线上，特别在此次新冠肺炎疫情期间，协同办公、在线教育、便民服务等领域移动应用积极助力复工复产，各地依托大数据推出“健康码”等疫情防控新举措，API 在其中起到了紧密链接各个元素的作用。为满足各领域移动应用业务需要，API 的绝对数量持续增长，通过 API 传递的数据量也飞速增长。API 技术借助移动应用蓬勃发展的势头融入社会经济的方方面面，不仅为数据交互提供了便利，并且推动了企业、组织机构间的沟通和对话，甚至创造了新的经济模式：API 经济。

（一）API 简介

API 是预先定义的函数，为程序之间数据交互和功能触发提供服务。调用者只需调用 API，并输入预先约定的参数，即可实现开发者封装好的各种功能，无需访问功能源码或理解功能的具体实现机制。

从功能角度来看，API 是前端调用后端数据的通道；从业务角度来看，API 是将封装后的应用对外开放的访问接口。在信息系统内部，随着业务功能的逐渐细化，各个功能模块之间需要利用 API 技术来进行协调；在信息系统外部，API 承担着与其他应用程序进行交互的

重要任务。

（二）API 分类及组成要素

1.API 分类

API 技术应用广泛，可满足不同领域、不同业务的数据传输和操作需求，在包括软件开发工具包（Software Development Kit，SDK）、Web 应用、网关等诸多领域均可发现 API 的身影。因此，从应用领域角度难以合理清晰地区分其种类。为此，本报告从 API 开放程度和 API 核心技术两个维度进行分类介绍。

（1）按 API 开放程度分类

从 API 的开放程度出发，API 可以分为开放 API、面向合作方 API 和内部 API。

开放 API 是面向公网开放的接口，此类 API 允许公众调用。调用者可以是任何人或者机构，不需要和 API 提供者建立合作关系，例如公司门户网站等。

面向合作方 API 指的是企业或组织用来与外部合作伙伴进行沟通、交流和系统集成的 API，例如面向外包机构、设备供应商等。

内部 API 仅在企业或组织内部使用，用来协调内部不同系统、应用之间的调用关系，例如 CRM 系统 API、薪资系统 API 等。

（2）按 API 核心技术分类

从 API 核心技术进行划分，可分为简单对象访问协议（Simple

Object Access Protocol，SOAP）API，RESTful（Representational State Transfer,REST)API 及远程过程调录(Remote Procedure Call，RPC）API。

SOAP API 是指使用 Web 服务安全性内置协议的 API。基于 XML 协议，此类 API 技术可与多种互联网协议和格式结合使用，包括超文本传输协议（HTTP）、简单邮件传输协议（SMTP）、多用途网际邮件扩充协议（MIME）等。

RPC API 是指使用远程过程调录协议进行编程的 API，RPC 技术允许计算机调用其他计算机的子系统，并定义了结构化的请求方式。

不同于上述两类依托于协议的 API 技术，RESTful API 是一种架构，其通过 HTTP 和 JSON 进行传输，不需要存储或重新打包数据，同时支持 TLS 加密。

2.API 组成要素

API 通常包含如下组成要素，在这些要素的共同作用下，API 才能发挥预期作用。

（1）**通信协议：**API 一般利用 HTTPS 等加密通讯协议进行数据传输，以确保数据交互安全。

（2）**域名：**用于指向 API 在网络中的位置。API 通常被部署在主域名或者专用域名之下，接入方可通过域名调用相关 API。

（3）**版本号：**不同版本的 API 可能存在巨大差异，尤其对于多版本并存、增量发布等情况，API 版本号有助于准确区分 API 的参数

设置。

（4）**路径：**路径又称“终点”（end point），指表示 API 及 API 执行功能所需资源的具体地址。

（5）**请求方式:**API 常用的请求方式有 GET、POST、PUT 和 DELETE 四种，分别用于获取、更新、新建、删除指定资源。

（6）**请求参数：**即传入参数，包含数据格式、数据类型、可否为空以及文字描述等内容。传入参数主要包括 Cookie、Request header、请求 body 数据和地址栏参数等。

（7）**响应参数：**即返回参数或传出参数，返回参数本身默认没有值，用于带出请求参数要求 API 后台所返回的数据。

（8）**接口文档：**接口文档是记录 API 相关信息的文档，内容包括接口地址、请求方式、传入参数（请求参数）和响应参数等。

（三）API 安全标准化情况

近年来，我国陆续出台多部数据接口有关标准，对数据接口在不同领域的应用、部署、管理、防护等进行了规范。

在国家标准层面，我国多部现行及制定中的国家标准针对 API 安全提出了安全要求。GB/T 35273-2020《信息安全技术 个人信息安全规范》将 API 开发、调用与个人信息安全相结合，明确指出“个人信息控制者在提供产品或服务的过程中部署了收集个人信息的第三方插件（例如网站经营者与在其网页或应用程序中部署统计分析工具、软件开发工具包 SDK、调用地图 API 接口），且该第三方并未

单独向个人信息主体征得收集、使用个人信息的授权同意，则个人信息控制者与该第三方为共同个人信息控制者。”制定中的国家标准 GB/ XXXX-XX《信息安全技术 政务信息共享 数据安全技术要求》要求共享交换过程中涉及的授权方（共享数据提供方、共享交换服务方）“支持资源文件、库表、接口等各共享方式上不同粒度的权限控制”，并在级联接口安全方面要求“共享交换服务方应采用密码技术对共享交换系统间的级联接口进行安全防护，保障通过级联接口传递的数据的保密性和完整性。”

表 1 相关国家标准例举

序号	标准编号	标准名称
1	GB/T 35273-2020	《信息安全技术 个人信息安全规范》
2	GB/T 36478.4-2019	《物联网 信息交换和共享 第 4 部分：数据接口》
3	GB/T 21062.3-2007	《政务信息资源交换体系 第 3 部分：数据接口规范》
4	GB/T 19581-2004	《信息技术 会计核算软件数据接口》
5	GB/ XXXX-XX	《信息安全技术 政务信息共享 数据安全技术要求（征求意见稿）》

来源：中国信息通信研究院

在通信行业标准方面，随着云计算、移动互联网等领域的快速发展，通信行业针对特定 API 类型、API 应用场景等制定了一系列标准，细化了 API 相关安全要求与规范。其中 YD/T 2807.4-2015《云

资源管理技术要求 第 4 部分：接口》对涉及的接口类型进行了梳理，规定了云资源管理平台及分平台间接口的技术要求。YD/T 3217-2017《基于表述性状态转移（REST）技术的业务能力开放应用程序接口（API）视频共享》则针对基于 REST 技术的视频共享能力开放 API 进行了规范，涵盖了接口资源定义、资源操作、数据结构、基本流程和安全要求等多方面内容。

表 2 相关通信行业标准例举

序号	标准编号	标准名称
1	YD/T 3420.8-2019	《基于公用电信网的宽带客户网关虚拟化 第 8 部分:接口要求》
2	YD/T 3496-2019	《Web 安全日志格式及共享接口规范》
3	YD/T 3242-2017	《生物灾害防治和预警系统 信息发布网络接口技术要求》
4	YD/T 3217-2017	《基于表述性状态转移（REST）技术的业务能力开放应用程序接口（API）视频共享》
5	YD/T 2406-2017	《互联网数据中心和互联网接入服务信息安全管理系统及接口测试方法》
6	YD/T 3215-2017	《互联网资源协作服务信息安全管理系统及接口测试方法》
7	YD/T 3214-2017	《互联网资源协作服务信息安全管理系统接口规范》

8	YD/T 3213-2017	《内容分发网络服务信息安全管理系统及接口测试方法》
9	YD/T 3212-2017	《内容分发网络服务信息安全管理系统接口规范》
10	YD/T 3189-2016	《基于表述性状态转移（REST）技术的业务能力开放应用程序接口（API）状态呈现业务》
11	YD/T 2807.4-2015	《云资源管理技术要求 第4部分:接口》
12	YD/T 2464-2013	《基于表述性状态转移（REST）技术的业务能力开放应用程序接口（API）搜索业务》
13	YD/T 1661-2007	《基于互联网服务（Web Service）的开放业务接入应用程序接口（Parlay X）技术要求》
14	YD/T 1262-2003	《开放业务接入应用程序接口（PARLAY API）技术要求》

来源：中国信息通信研究院

在金融行业标准方面，已发布多部标准对 API 技术的部署、管理进行规范。其中 JR/T 0171-2020《个人金融信息保护技术规范》要求金融机构嵌入或接入 API 时，应符合相应技术规范要求，进行检查、评估和审计。JR/T 0185—2020《商业银行应用程序接口安全管理规范》则对 API 技术提出了包括数据完整性保护、授权管理、

使用情况监控、接口访问日志留存、安全密钥管理、网络安全防护措施部署、接口安全监测、接口调用控制、接口变更处理、应急处理方案、安全审计溯源等一系列安全要求。

表 3 相关金融行业标准例举

序号	标准编号	标准名称
1	JR/T 0185-2020	《商业银行应用程序接口安全管理规范》
2	JR/T 0171-2020	《个人金融信息保护技术规范》
3	JR/T 0160-2018	《期货市场客户开户数据接口》
4	JR/T 0155.1-2018	《证券期货业场外市场交易系统接口 第 1 部分：行情接口》
5	JR/T 0155.2-2018	《证券期货业场外市场交易系统接口 第 2 部分：订单接口》
6	JR/T 0155.3-2018	《证券期货业场外市场交易系统接口 第 3 部分：结算接口》
7	JR/T 0151-2016	《期货公司柜台系统数据接口规范》
8	JR/T 0109.2-2015	《智能电视支付应用规范 第 2 部分：报文接口规范》
9	JR/T 0109.4-2015	《智能电视支付应用规范 第 4 部分：通信接口规范》
10	JR/T 0078-2014	《银行间市场数据接口》

11	JR/T 0096.1-2012	《中国金融移动支付 联网联合 第 1 部分：通信接口规范》
12	JR/T 0087-2012	《股指期货业务基金与期货数据交换接口》
13	JR/T 0055.5-2009	《银行卡联网联合技术规范 第 5 部分：通信接口》
14	JR/T 0024-2004	《国际收支统计间接申报银行接口规范 通用要素》

来源：中国信息通信研究院

在交通行业标准方面，也相继出台了包括 JT/T 1183-2018《出租汽车 ETC 支付接口规范》、JT/T 1049-2017《道路运政管理信息系统》在内的多部 API 相关标准和规范性文件。

表 4 相关交通行业标准例举

编号	标准编号	标准名称
1	JT/T 1183-2018	《出租汽车 ETC 支付接口规范》
2	JT/T 1049-2017	《道路运政管理信息系统》
3	JT/T 1049.5-2017	《道路运政管理信息系统第 5 部分：省级业务系统接口》
4	JT/T 1019.3-2016	《12328 交通运输服务监督电话系统 第 3 部分：数据交换与信息共享接口技术要求》
5	JT/T 1049.2-2016	《道路运政管理信息系统第 2 部分:数

		据资源采集接口》
6	JT/T 1049.3-2016	《道路运政管理信息系统第 3 部分:数据资源目录服务接口》
7	JT/T 979.1-2015	《道路客运联网售票系统 第 1 部分：服务接口规范》
8	JT/T 785-2010	《道路运输管理与服务系统数据交换接口》

来源：中国信息通信研究院

二、近年来 API 安全态势

API 在互联网时代向大数据时代快速过渡的浪潮中承担着连接服务和传输数据的重任，在通信、金融、交通等诸多领域得到广泛应用。API 技术已经渗透到了各个行业，涉及包含敏感信息、重要数据在内的数据传输、操作，乃至各种业务策略的制定环节。伴随着 API 的广泛应用，传输交互数据量飞速增长，数据敏感程度不一，API 安全管理面临巨大压力。

近年来，国内外已发生多起由于 API 漏洞被恶意攻击或安全管理疏漏导致的数据安全事件，对相关企业和用户权益造成严重损害，逐渐引起各方关注。为此，部分企业已经积极采取改进 API 安全策略、出台替代方案等防护措施，应对日益严峻的安全形势。

（一）Facebook 多起数据泄露事件与 API 有关

2018 年 9 月，黑客利用 Facebook 某 API 安全漏洞获取数百万用

户信息。Facebook 提供“View As”功能允许开发者以用户身份查看页面，由于相关 API 存在安全漏洞，造成大量用户访问口令（Access Token）泄露，并导致大量用户个人信息被不法分子窃取，近 5000 万用户受到影响。

2018 年 12 月，Facebook 再次曝出 API 漏洞导致用户个人信息泄露事件，影响近 680 万用户及 1500 个使用该 API 的 App。该漏洞允许第三方 App 访问用户 Facebook 账户内未公开的照片，App 还可能利用该漏洞在用户访问中断或退出程序后获取用户设备缓存中的数据。

2019 年 12 月，国外安全人员发现超过 2.67 亿条 Facebook ID、电话号码和姓名等信息被储存在某公开数据库中。有研究显示，该数据库中的数据可能通过某未知 API 接口抓取，并非来自用户公开信息。Facebook 称将对这一事件展开调查。

（二）美国邮政服务 API 漏洞导致用户信息泄露

2018 年，国外研究人员发现美国邮政服务（USPS）API 漏洞可能导致超过 6000 万用户个人信息被窃取。出现漏洞的“Informed Visibility”接口旨在为 USPS 旗下运输业务提供实时跟踪数据，但由于未设置如限速限流在内的防护措施，使得这一 API 接口遭到不法分子滥用。

（三）T-Mobile API 漏洞导致用户账号被窃取

2019 年 11 月，美国电信运营商 T-Mobile 曝出 Web 应用程序界

面漏洞。不法分子通过该漏洞窃取了 T-Mobile 用户电子邮箱地址、设备识别信息、安全问题答案等信息，进而利用非法获取的信息冒充客户挂失手机 SIM 卡，接管受害者电话服务，并通过该手机号码绑定的双重认证、账户恢复等功能非法访问或窃取用户账号。约 1500 万 T-Mobile 用户受到影响。

（四）Twitter 虚假账户利用 API 批量匹配用户信息

2019 年 12 月 24 日，Twitter 公司发现大量虚假账户非法调用提供电话号码搜索用户功能的 API 接口。不法分子可利用这一接口获取用户信息，进而开展钓鱼攻击、电话诈骗等违法活动。Twitter 于事件曝光后紧急修改该接口功能使相关查询无法返回具体的账户名称。

（五）考拉征信非法出售 API 导致个人信息泄露

2019 年 11 月，拉卡拉支付旗下的考拉征信因非法缓存公民个人信息、出售查询 API 遭警方调查。警方表示，经查考拉征信从上游公司获取接口后又违规将查询接口卖出，并利用查询接口非法缓存公民姓名、身份证号码和身份证照片等个人身份信息一亿多条，供下游公司查询牟利，从而造成公民身份信息包括身份证照片的大量泄露。案件发生后，警方已将考拉征信涉案人员抓获。

（六）新浪微博用户查询接口被恶意调用导致数据泄露

2020 年 3 月 19 日，媒体报道新浪微博因用户查询接口被恶意调用导致 App 数据泄露。新浪微博方面称此次数据泄露可追溯至 2018 年末，有用户非法调用 App 用户查询接口，通过批量上传手机通讯录匹配用户账号昵称，并结合其他渠道获取的信息进行出售。事件曝光后，新浪微博表示将采取升级接口安全策略等措施，做好用户个人信息保护工作。

（七）微信团队收回小程序"用户实名信息授权"接口

2020 年 3 月 31 日，腾讯微信团队在“微信开放社区”发布《关于收回小程序"用户实名信息授权"接口的相关说明》，称为进一步提升用户使用的安全体验，将于 2020 年 5 月 31 日收回小程序“用户实名信息授权”接口，并停止了该接口的申请和接入。微信方要求无相关业务场景或需求的小程序停止使用该接口，并向仍有用户实名认证需求的小程序提供“实名信息校验接口”作为替代方案。

三、安全风险分析

（一）外部威胁因素

从近年API 安全态势可以看出,API 技术被应用于各种复杂环境，其背后的数据一方面为企业带来商机与便利，另一方面也为数据安全保障工作带来巨大压力。特别在开放场景下，API 的应用、部署面向个人、企业、组织机构等不同用户主体，面临着外部用户群体庞大、性质复杂、需求不一等诸多挑战，需时刻警惕外部安全威胁。

1.API 漏洞导致数据被非法获取

在 API 的开发、部署过程中不可避免产生安全漏洞，这些漏洞通常存在于通信协议、请求方式、请求参数和响应参数等环节。不法分子可能利用 API 漏洞（如缺少身份认证、水平越权漏洞、垂直越权漏洞等）窃取用户信息、企业核心数据。例如在开发过程中使用非 POST 请求方式、Cookie 传输密码等操作登录接口，存在 API 鉴权信息暴露风险，可能使得 API 数据被非法调用或导致数据泄露。

2.API 成为外部网络攻击的重要目标

API 是信息系统与外部交互的主要渠道，也是外部网络攻击的主要对象之一。针对 API 的常见网络攻击包括重放攻击、DDoS 攻击、注入攻击、会话 cookie 篡改、中间人攻击、内容篡改、参数篡改等。通过上述攻击，不法分子不仅可以达到消耗系统资源、中断服务的目的，还可以通过逆向工程，掌握 API 应用、部署情况，并监听未加密数据传输，窃取企业数据。

3.网络爬虫通过 API 爬取大量数据

网络爬虫能够在短时间内爬取目标应用上的所有数据，常表现为某时间段内高频率、大批量进行数据访问，具有爬取效率高、获取数据量大等特点。通过开放 API 对 HTML 进行抓取是网络爬虫最简单直接的实现方式之一，不法分子通常采用假 UA 头和假 IP 隐藏身份，一但获取企业内部账户，可能利用网络爬虫获取该账号权限内的所有数据。如果存在水平越权和垂直越权等漏洞，在缺少有效的

权限管理机制情况，不法分子可以通过掌握的参数特征构造请求参数进行遍历，导致数据被全量泄露。此外，移动应用软件客户端数据多以 JSON 形式传输，解析更加简单，反爬虫能力更弱，更易受到网络爬虫威胁。

4.合作第三方非法留存接口数据

企业通过 API 实现与合作第三方之间数据交互的过程中，可能存在合作方恶意留存接口数据的风险。以个人身份验证类合作为例，在需要进行实名验证的时候，合作方可通过 API 请求调用相关个人身份信息。正常情况下，服务器获取请求后在后端进行验证并返回结果，此过程中恶意合作方可能留存验证结果，经过长时间积累，非法变相获取大量的个人身份信息资源，对企业数据库形成事实上的拖库。

5.API 请求参数易被非法篡改

不法分子可通过篡改 API 请求参数，结合其它信息匹配映射关系，达到窃取数据的目的。以实名身份验证过程为例，用户端上传身份证照片后，身份识别 API 提取信息并输出姓名和身份证号码，再传输至公安机关相应 API 进行核验，并输出认证结果。此过程中，不法分子可通过修改身份识别 API 请求参数中的姓名、身份证号码组合，通过遍历的方式获取姓名与身份证号码的正确组合。可被篡改的 API 参数通常有姓名、身份证号码、账号、员工 ID 等。此外，企业中员工 ID 与职级划分通常有一定关联性，可与员工其它信息形

成映射关系，为 API 参数篡改留有可乘之机。

（二）内部脆弱性因素

应对外部威胁的同时，API 也面临许多来自内部的风险挑战。一方面，传统安全通常是通过部署防火墙、WAF、IPS 等安全产品，将组织内部与外部相隔离，达到纵深防御的目的，但是这种安全防护模式建立在威胁均来自于组织外部的假设前提上，无法解决内部隐患。另一方面，API 类型和数量随着业务发展而扩张，通常在设计初期未进行整体规划，缺乏统一规范，尚未形成体系化的安全管理机制。因此，从内部脆弱性来看，影响 API 安全的因素主要包括以下几方面。

1. 身份认证机制

身份认证是保障 API 数据安全第一道防线。一方面，若企业将未设置身份认证的内网 API 接口或端口开放到公网，可能导致数据被未授权访问、调用、篡改、下载。不同于门户网站等可以公开披露的数据，部分未设置身份认证机制的接口背后涉及企业核心数据，暴露与公开易引发严重安全事件。另一方面，身份认证机制可能存在单因素认证、无口令强度要求、密码明文传输等安全隐患。在单因素身份验证的前提下，如果口令强度不足，身份认证机制将面临暴力破解、撞库、钓鱼、社会工程学攻击等威胁。如果未对口令进行加密，不法分子则可能通过中间人攻击获取接口认证信息。

2.访问授权机制

访问授权机制是保障 API 数据安全的第二道防线。用户通过身份认证即可进入访问授权环节，此环节决定用户是否有权调用该接口进行数据访问。系统在识别用户之后，会根据权限控制表或权限控制矩阵判断该用户的数据操作权限。常见的访问权限控制策略有三种，基于角色的授权（Role-Based Access Control）、基于属性的授权（Attribute-Based Access Control）以及基于访问控制表授权（Access Control List）。访问授权机制风险通常表现为用户权限大于其实际所需权限，从而该用户可以接触到本无权访问的数据。导致这一风险的常见因素包括授权策略选择不恰当、授权有效期过长、未及时收回权限等。

3.数据脱敏策略

除了为不同的业务需求方提供数据传输以外，为前端界面展示提供数据支持也是 API 的重要功能之一。API 数据脱敏策略通常可分为前端脱敏和后端脱敏。前者指数据被 API 传输至前端后再进行脱敏处理；后者则相反，API 在后端完成脱敏处理，再将已脱敏数据传输至前端。如果未在后端对个人敏感信息等数据进行脱敏处理，且未加密传输，一旦流量被截获、破解，将对企业、公民个人权益造成严重影响。此外，未脱敏数据在传输至前端时，如被接收方终端缓存，也可能导致敏感数据暴露。而脱敏策略不统一可能导致相同数据脱敏部分不同，不法分子可通过拼接方式获取原始数据，造成

脱敏失效。

4.返回数据筛选机制

如果 API 缺乏有效的返回数据筛选机制，可能由于返回数据类型过多、数据量过大等因素形成安全隐患。首先，部分 API 设计初期未根据业务进行合理细分，未建立单一、定制化接口，使得接口臃肿、数据暴露面过大。其次，在安全规范欠缺和安全需求不明确的情况下，API 开发人员可能以提升速度为目的，在设计过程中忽视后端服务器返回数据的筛选策略，导致查询接口会返回符合条件的多个数据类型，大量数据通过接口传输至前端并进行缓存。如果仅依赖于前端进行数据筛选，不法分子可能通过调取前端缓存获取大量未经筛选的数据。

5.异常行为监测

异常访问行为通常指非工作时间访问、访问频次超出需要、大量敏感信息数据下载等非正常访问行为。即使建立了身份认证、访问授权、敏感数据保护等机制，有时仍无法避免拥有权限的用户进行数据非法查询、修改、下载等操作，此类访问行为往往未超出账号权限，易被管理者忽视。异常访问行为通常与可接触敏感数据岗位或者高权限岗位密切相关。如负责管理客户信息的员工可能通过接口获取用户隐私信息出售谋利；即将离职的高层管理人员可能将大量公司机密和敏感信息带到下一家公司，以在商业竞争中占据优势等。美国执法机构和网络安全监管机构调查结果显示超过 85%的安

全威胁来自企业内部，企业必须高度重视可能由内部人员引发的数据安全威胁。

6.特权账号管理

从数据使用的角度来说，特权账号指系统内具有敏感数据读写权限等高级权限的账号，涉及操作系统、应用软件、企业自研系统、网络设备、安全系统、日常运维等诸多方面，常见的特权账号有 admin、root、export 账号等。除企业内部运维管理人员外，外包的第三方管理人员、临时获得权限的设备原厂工程人员等也可能使用特权账号。多数特权账号可通过 API 进行访问，有心者可能以特权账号非法查看、篡改、下载企业数据。此外，部分企业出于提升开发运维速度的考虑会在团队内共享账号，并允许不同的开发运维人员从各自终端登陆并操作，一旦发生数据安全事件，难以快速定位责任主体。

7.第三方管理

当前，需要共享业务数据的应用场景日益扩展，第三方调用 API 访问企业数据完成业务工作的同时，也成为了企业的安全短板。尤其对于涉及个人敏感信息或重要数据的 API，如果企业忽视对第三方进行风险评估和有效管理、缺少对其数据安全防护能力的审核，一旦第三方存在安全隐患或不法企图，可能发生数据被篡改、泄露、甚至非法贩卖等安全事件，对企业数据安全、社会形象乃至经济利益造成影响。

四、安全建议

API 安全是当今时代数据安全保护的重要一环。企业应在把握自身现状的基础上梳理 API 相关安全风险，建立健全 API 安全管理制度，针对事前、事中和事后各阶段管理和技术需求差异，部署相应安全措施，加强数据安全风险防范。

（一）事前

1.统一 API 设计开发规范，减少安全隐患

缺乏统一规范、开发维护不当导致的安全漏洞等脆弱性因素可能为 API 带来严重安全隐患。建议企业建立健全 API 设计、开发、测试等环节标准规范和管理制度，引导 API 开发运维流程标准化，提高对 API 安全的重视程度，将相关要求以制度规程等形式进行沉淀、落实，避免遗留严重安全漏洞、恶性 bug 等脆弱性因素，威胁接口安全。

2.强化 API 上线、变更、下线环节实时监控，确保全生命周期安全

API 全生命周期包括 API 上线、变更和下线三个环节。企业应对自身 API 部署情况进行全面排查，梳理统计 API 类型、活跃接口数量、失活接口数量等资产现状，针对 API 上线、运行中变更、失活后下线等环节进行实时监控。企业应在新 API 上线前进行风险评估，发现问题暂停上线并及时调整，确保上线 API 安全性；上线后应对

其运行情况进行实时监控，发现接口运行异常、恶意调用等情况及时采取防护措施，修复相应问题；若 API 不再使用，企业应遵循下线流程及时进行处理，防止失活 API 持续在线，成为安全隐患。

3.完善 API 身份认证和授权管理机制，强化接口接入安全审核

企业应针对除信息公开披露场景以外的 API 建立有效的身份认证机制，对现有身份认证机制密码强度、双因素认证、密码更新等安全要素进行评估，健全身份认证机制；在建立有效的身份认证基础上，建立健全访问授权机制，严格遵循最小必要权限原则，尤其针对提供数据增、删、改等高危操作的 API，严格规范用户权限管理；对涉及敏感信息、重要数据的 API 加强接入方资质和数据安全防护能力审核，规范合作要求，避免因接入方原因导致数据安全事件。

4.健全 API 安全防护体系，提升抵御外部威胁能力

企业应加强 API 安全防护能力建设，针对重要接口部署专门的防护设备保障其安全，建立健全安全防护体系。具体措施包括但不限于部署 API 网关统一接口管理；利用 VPN 等加密通道传输数据；部署应用防护系统保护 Web 应用；建立 API 访问白名单机制；部署抗 DDoS 工具等。从而提升企业 API 抵御外部威胁的能力，降低数据安全事件发生几率。

5.加大 API 安全保护宣传力度，提高员工安全意识

企业应加大对 API 安全保护的宣传力度，缩小各部门之间对 API 安全重视程度差异，提高员工特别是 API 开发运维人员的安全意识，进一步提高企业整体数据安全认识。推动 API 保护相关机制、技术手段落地，避免因 API 安全管理疏漏等内部因素导致数据泄露、丢失、损毁等安全事件，对企业业务发展、社会形象造成负面影响。

（二）事中

1.加强 API 身份认证实时监控能力建设

企业应加强 API 身份认证实时监控能力建设，重点监控高频登录尝试、空 Referer、非浏览器 UA 头登录等具有典型机器行为特征的操作，对异常登录、调用行为进行分析，发现恶意行为及时告警。此外，企业应实时监控接口运行中的单因素认证、弱密码、密码明文传输等脆弱性问题，建立账号登录行为画像，形成用户常规登录特征基线，对不同 IP 登录、连续认证失败、境外 IP 访问等敏感操作进行监测分析，发现账号共享、借用、兼任等违规行为及时对相关账号操作进行限制、阻断，避免安全事件的发生或扩大。

2.加强异常行为实时监测预警能力建设

企业应加强异常访问行为监测能力建设，针对短时间内大量获取敏感数据、访问频次异常、非工作时间获取敏感数据、敏感数据外发等异常调用、异常访问行为进行实时监测分析，根据自身业务

情况建立正常行为基线，防范内部违规获取数据、外部攻击或网络爬虫等数据安全风险。此外，由于内部特权账号权限远超普通用户账户，企业应针对此类账号建立实时行为监测和审计机制，对账号异常、高危操作进行严格管控，建立精准、细化的特权账号行为基线，及时对特权账号异常行为进行预警，并定期进行特权帐号安全审计。

3.加强数据分类分级管控能力建设

企业应梳理 API 数据类型，落实数据分类分级管控措施，针对 API 涉及的敏感数据按照统一策略进行后端脱敏处理,并结合数据加密、传输通道加密等方式保护 API 数据传输安全。企业应严格落实敏感数据保护策略，部署敏感数据监测工具，及时发现未脱敏展示、前台脱敏等现象，并对接口流量进行分析，杜绝敏感数据明文传输等违规行为。企业应评估涉及敏感数据的 API 参数设置情况，重点关注接口单次返回数据量过多、返回数据类型过多等情况，建立后端数据量、数据类型筛查机制，确保敏感数据暴露可知、可控、可追溯。

4.加强 API 数据流向监控能力建设

企业应建立 API 数据流量监测机制，实时监控数据流向，加强数据流向监控能力建设。通过分析访问和被访问 IP 的局域、地域或法域，实现对数据流向的实时监控，防范数据接收方非法出售或滥用个人信息风险，发现相关违法违规事件及时阻断 API 接入，为后

续溯源调查积极存证。此外，企业应对境外 IP 访问内网 API 或者内部 IP 访问境外 API 的情况重点关注、及时预警，确保敏感数据出境活动合法合规。

（三）事后

1. 建立健全应急响应机制

当前 API 应用广泛，业务逻辑复杂，涉及数据量大，一旦发生安全事件，可能给企业、用户带来严重影响。企业应严格落实《网络安全法》《电信和互联网用户个人信息保护规定》（工信部第 24 号令）等法律法规要求，出现数据泄露等严重安全事件及时告知相关用户并上报电信主管部门，制定 API 安全事件应急响应预案并纳入企业现有应急管理体系，应急流程包括但不限于监测预警及报告、数据泄露事件处置、危机处理及信息披露等环节。

2. 建立健全日志审计机制

API 数据安全审计可以帮助企业有效识别具体的高危访问行为，为企业 API 安全提供有力帮助。建议企业对接口访问、数据调用等操作进行完整日志记录，并定期开展安全审计，对 API 安全进行回顾，结合旁路 API 流量捕获等技术手段，对传输协议等安全要点进行分析还原，识别 API 漏洞、异常调用、外部攻击等安全风险。同时，建议企业根据安全审计结果编制审计报告，跟踪审计意见的后续落实，并依据相关监管要求妥善保存日志信息等，为安全事件追

溯提供依据。

3. 建立健全数据泄露溯源追责机制

企业应建立健全数据泄露溯源追责机制，制定 API 相关安全事件溯源方案，发生安全事件后及时追踪数据泄露途径、类型、规模、原因，分析根本原因，提取有效证据。结合审计机制进行事件溯源，在确定责任主体后，严肃问责。API 数据泄露溯源机制可分为线索溯源和主体溯源，线索溯源以泄露数据内容为线索，在系统中进行回溯，提取 API 日志中的相关记录进行分析，确实责任人和泄露路径；主体溯源根据账号、接口信息等访问特征线索在日志流量信息中进行筛选，分析匹配特征，追溯事件源头。由于传统人工溯源费时费力，溯源结果准确度有限，建议企业结合自身需求部署自动化溯源工具，提升溯源效率，为企业 API 安全管理提供助力。

五、附录

（一）全知科技 API 安全实践

1.开放 API 安全实践

（1）场景简介

开放 API 将接口开放到公网，为不同用户、产品提供数据操作、传输渠道。开放 API 可分为两类，**一类**通过网页交互即可调用后端 API 进行数据查询，例如企业门户网站；**一类**仅对注册用户开放，需用户主动注册后才可调用，例如政务开放平台数据调用接口。此类 API 主要具有两大特点。**一是接口对社会公众开放。**只要获知 URL 链接，任何人都可以对 API 进行访问，而调用 API 接口即代表着调用 API 背后不同的业务功能，获取不同的服务数据。**二是 API 参数由数据提供方进行定义。**全面开放的 API 通常无法满足所有用户的访问需求，为了业务的正常开展，通常需进行标准化的接口定制。

（2）安全方案

企业应全面梳理其开放 API 现状，了解开放 API 数量、性质、活跃程度，确保没有内网接口开放到外网的情况，并关注活跃 API 数据调用情况是否存在异常，及时下线失活 API。

在此基础上，企业可采用多种技术手段保护 API 安全，降低安全风险。**一是**对 API 进行生命周期监控，**二是**健全账号认证机制和授权机制，**三是**实时监控 API 账号登录异常情况，**四是**执行敏感数

据保护策略，**五是**建立接口防爬虫防泄漏保护机制。

来源：全知科技（杭州）有限责任公司

API 生命周期监控：企业需实时监控新 API 上线、API 在运行过程中变更，API 失活后正确下线情况，并在新 API 上线前对其进行风险评估，对通信协议、路径、请求方式、请求参数、响应参数等要素中的潜在安全漏洞进行排查，发现可能被攻击导致数据泄露的安全漏洞，应及进行调整，确保上线前的安全性和可靠性。API 上线后，企业则需实时监控其运行状态，发现风险应及时修正后再重新上线。若 API 由于业务更迭等情况不再使用，企业应按照正确流程对其进行下线。

健全认证授权机制：首先，企业需排查缺少身份认证的高危开放 API，并对其建立身份认证机制。其次，企业应采取强密码、双因素认证等方式增强身份认证机制。此外，在身份认证的基础上，企业应建立健全授权机制，对用户账号授予所需最小权限，尤其注意

增、删、改等高危操作，如无必要，不授予系统管理员 admin 或 export 等高级权限。建立健全认证授权机制一方面可以确保数据调用方为真实用户而非网络爬虫，另一方面可以保证用户访问记录可追溯。

登录异常行为监控：企业应建立 API 异常登陆实时监控机制，监测账号异常登陆情况并及时预警。账号异常登录情况可能由账号暴力破解、撞库、单因素认证等登录系统脆弱性导致。登陆异常情况监控机制可对接口登陆方式、IP 登陆失败频率、失败原因等进行分析，发现异常情况及时预警。

敏感数据保护策略：企业应对开放 API 涉及的敏感数据进行梳理，在分类分级后按照相应策略进行脱敏展示，所有敏感数据脱敏均在后端完成，杜绝前端脱敏。此外敏感数据需通过加密通道进行传输，防止传输过程中的数据泄露。以金融类系统为例，客户端应用软件、银行卡受理设备、自助终端设备等界面展示的个人金融信息需进行脱敏处理，确保登陆系统前不展示敏感信息。在此基础上，企业应部署敏感数据监测工具，实时监测前端界面是否存在敏感数据明文显示，以及通过流量分析检测是否存在敏感数据明文传输，验证是否有效执行敏感数据保护策略。

部署防爬虫、防泄漏保护机制：企业应部署接口防爬虫、防泄漏保护机制，分析用户访问行为特征，辨别该访问是真实用户行为还是机器行为，并根据网络爬虫特征制定监控策略，部署工具进行实时监控预警，发现潜在数据泄露事件及时触发熔断机制，阻断网络爬虫行为对 API 数据安全的威胁。

2.面向合作方 API 安全实践

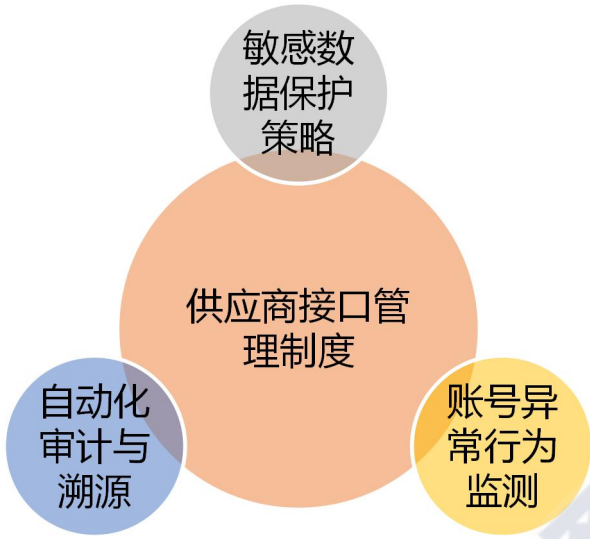
（1）场景简介

商业生态系统的建立涉及企业与顾客、市场媒介、供应商等各方的合作互动，面向合作方 API 被广泛用于合作方之间的数据交互共享。此类 API 主要具有 3 大特点。**一是数据交换类型多。**通过此类 API 进行数据交换的多为企业合作伙伴，包括但不限于资源供应商和服务提供商。**二是数据交换参与方数量少。**开放 API 用户一般以个人居多，组织较少，而面向合作方的 API 调用则以组织居多，个人较少。**三是接口定义需双方协商。**此类 API 需在满足业务要求的前提下根据双方要求进行自定义，往往需预留等多种接口以满足业务需求。

（2）安全方案

企业应建立完善的供应商接口管理制度，包括准入制度、授权管理制度和退出制度等，约束企业与合作方间的合作，从源头上对合作方 API 进行把控，预防数据安全风险。在合作结束后，企业应及时下线相关接口，并按照合作协议要求，进行数据留存审计，确保合作方完成数据删除和销毁。

此外，企业还可通过部署相关技术手段保护面向合作方的 API 安全。**一是**部署敏感数据保护策略，**二是**建立账号异常行为监测机制，**三是**部署自动化审计与溯源工具。



来源：全知科技（杭州）有限责任公司

敏感数据保护策略：企业应对数据交换过程中涉及的敏感数据制定保护策略，并通过脱敏、匿名化、去标识化、数据加密、传输通道加密等方式对敏感数据加以保护。同时，组织机构还可以选择 VPN 传输、专线传输等安全性更高的安全防护手段，保护 API 接口数据安全。

账号异常行为监测：企业应建立账号异常行为风险监测机制，根据业务实际情况制定监控策略，实时监控合作方账号操作行为，一旦监测发现存在越权操作、非工作时间访问、非工作时间大量获取数据等情况，及时预警，降低数据安全事件风险。

自动化审计与溯源：企业与合作方之间通过 API 进行数据分享频繁，流动数据量大。一方面企业应通过系统日志准确记录和保存接口数据共享的情况，定期审计，及时发现数据交换中存在的风险。另一方面企业应部署自动化审计和溯源工具，对安全事件快速溯源、精准定位，防止数据泄露，保护企业数据安全。

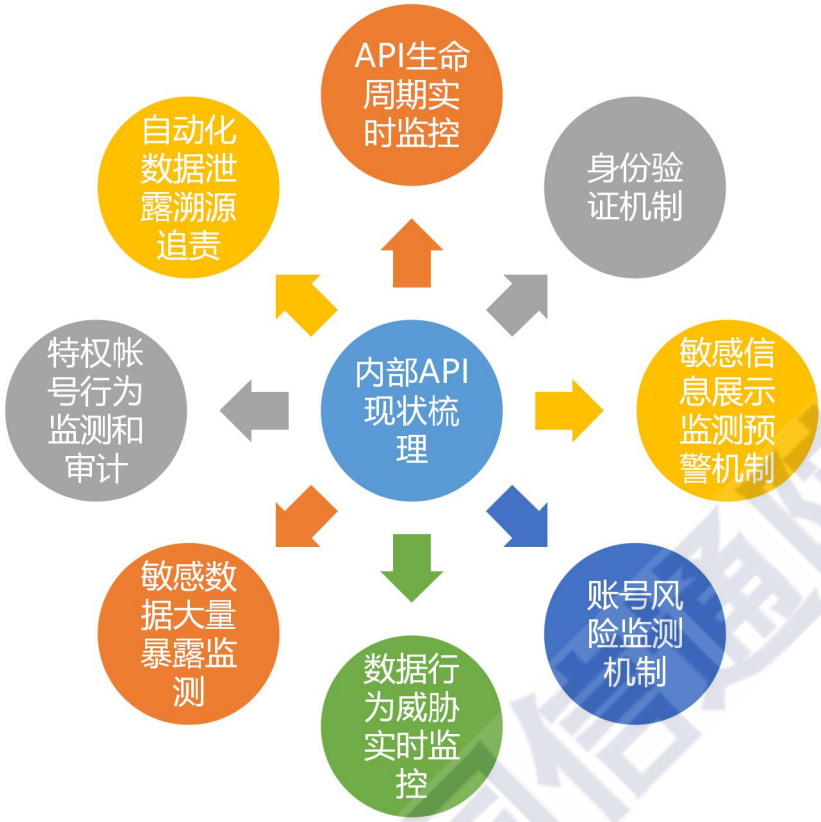
3.内部 API 安全实践

（1）场景简介

除了开放到公网、面向合作方的 API 之外，企业内部的应用系统通常也会通过内部 API 进行数据访问。此类 API 主要有 3 大特点。**一是众多应用系统衍生大量接口。**企业内部存在众多应用系统，根据业务功能的划分和用户群体的不同可能会衍生出诸多内部 API 接口。**二是接口调用群体庞杂。**企业内部员工因所处的部门和层级不同，存在不同业务需求和权限，造成 API 调用群体庞杂，为安全管理带来一定挑战。**三是接口参数由企业根据自身需求进行定义。**企业内部可能存在多种 API，需要根据内部人员对于业务功能的需求分别进行定义。

（2）安全方案

与开放 API 接口一样，企业应梳理内部 API 现状，围绕内部 API 生命周期建立有效管理机制。内部 API 接口可能随内部业务频繁迭代，企业也会引入新的系统或设备到内部网络，此时需额外关注内部 API 的安全要求。此外，企业还应部署或强化相应技术手段对内部 API 接口进行保护。**一是** API 生命周期实时监控，**二是**加强身份验证机制，**三是**建立敏感信息展示监测预警机制，**四是**建立账号风险监测机制，**五是**数据行为威胁实时监控，**六是**敏感数据大量暴露监测，**七是**特权账号行为实时监测和审计机制，**八是**自动化数据泄露溯源追责。



来源：全知科技（杭州）有限责任公司

API 生命周期实时监控：企业应在掌握内部接口现状的基础上，在新 API 上线前进行安全评估，严格内部 API 接口变更管理，对失活接口及时处理。接口现状发生改变应及时发布预警，并及时响应和处理。

身份验证机制：身份认证是企业数据安全的第一道防线，企业应从安全需求、成本和系统兼容性等方面进行综合考虑，选择如双因素认证、强密码口令、生物识别信息等认证措施，完善内部 API 身份验证机制。

敏感信息展示监测预警机制：企业应在确保脱敏策略一致的基础上，建立敏感信息明文展示监测预警机制，对内部 API 调用流量进行实时监控，一旦监测到明文传输敏感信息、或者明文展示敏感

信息的时候，及时进行预警。

账号风险监测机制：企业应建立账号风险监测机制。一方面，监测是否存在单因素认证、弱密码、密码明文传输等脆弱性；另一方面，建立账号登陆行为画像，总结用户常规登陆模式，发现账号共享、借用、兼任等情况及时预警，并进一步排查。此外，账号风险监测机制还可侦测境外 IP 访问内部 API 接口的情况，减少企业数据出境的安全风险。

数据行为威胁实时监控：内部 API 可能存在水平越权、垂直越权、账号滥用等风险，因此，企业应根据自身情况建立正常行为基线，对短时间内大量获取敏感数据、访问频次异常、非工作时间访问、敏感数据外发等异常行为进行监测，并防范网络爬虫等大量机器拉取内部数据。

敏感数据大量暴露监测：企业应监测 API 接口单次返回敏感数据量、敏感数据类型等情况，发现异常及时对接口进行改进。

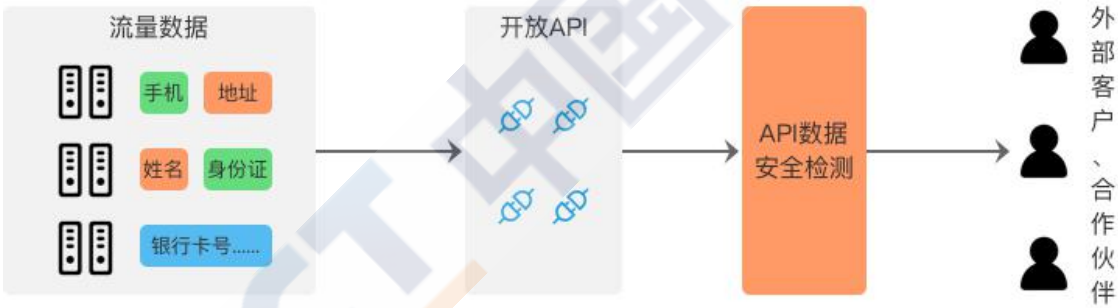
特权账号行为监测和审计：企业应建立并严格执行特权账号行为监测和审计机制，精确、细化特权账号行为基线。

自动化数据泄露溯源追责：通过线索溯源或者主体溯源模式进行溯源追责，明确数据泄露途径、数据泄露类型、数据泄露规模和数据泄露原因，并对源头责任人和可疑犯罪人进行锁定，及时缩小犯罪嫌疑人范围，减少因数据泄露给企业、个人和社会造成的负面影响。

（二）观安 API 安全实践

1. 安全方案

观安 API 数据安全检测方案通过对数据接口、虚拟网络边界接口进行实时监控和分析，实现应用系统之间数据访问、传输、流转及敏感数据检测，利用大数据分析技术构建数据接口活动轨迹、访问操作画像，智能化判断业务系统、企业内外部数据接口之间的数据流量异常、数据访问操作异常、数据接口调用异常等安全风险，及时对数据接口异常事件进行预警，为应用系统业务数据安全流转、调用、传输等操作访问行为提供数据安全保障。



来源：上海观安信息技术股份有限公司

一是梳理接口敏感级别，制定分级策略。梳理并发现应用系统中涉及敏感数据流转的接口以及敏感数据暴露面，根据敏感数据类型对应用系统接口进行敏感等级划分，针对不同敏感级别的接口制定差异化访问控制策略。

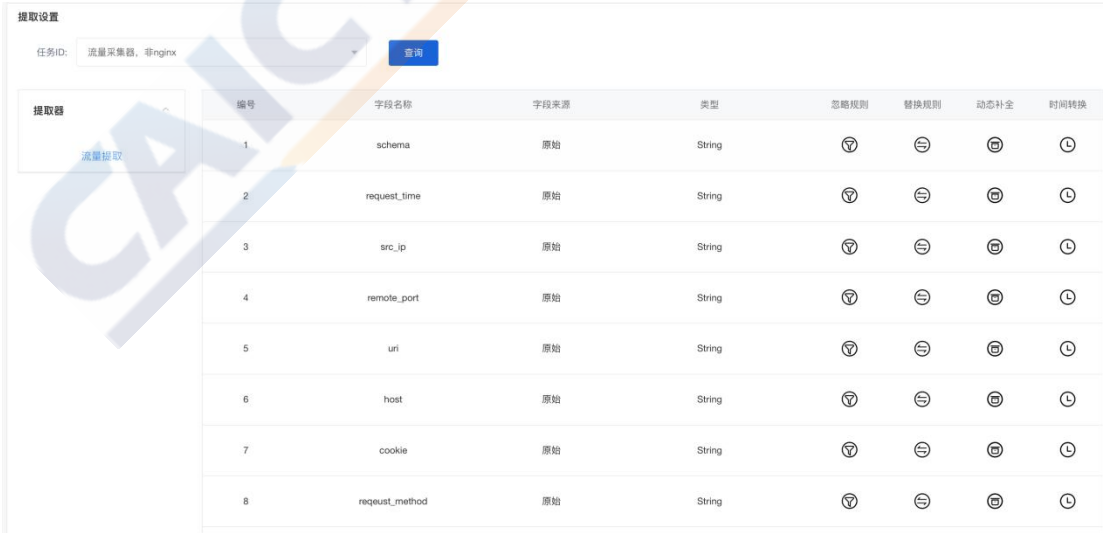
二是建立深度分析系统，实现多维度风险评估。建立深度分析系统，对数据接口异常流量、用户异常操作行为、异常调用等进行实时监控、异常预警和集中的风险展示。对敏感数据访问接口进行

多维度的脆弱性评估及风险识别，包括但不限于数据账号风险、数据权限风险、数据操作风险、数据流向风险、数据暴露面风险、数据脱敏风险等。

三是描绘行为轨迹，实现流动监控。基于流量数据识别应用系统中的接口和用户账号信息，还原并记录用户的数据访问行为；对业务系统账号信息的数据访问行为进行审计，从用户账户、接口、数据访问和返回情况，完整描绘数据在应用系统中流转的地图，实现对数据流动细节的监控。

2. 技术手段

协议解析：通过获取网络中系统的数据包，并将其进行协议解析，生成基础数据，识别的协议包括但不限于当前主流的系统访问及接口协议。通过抓取的流量数据可对数据流动使用过程进行审计操作，保证 API 内的数据流转安全性。



来源：上海观安信息技术股份有限公司

数据分类分级：分类分级定位到的数据标签信息、位置信息可

以赋能到安全风险识别，结合流量数据准确实时的输出安全风险告警，保障数据生命周期内的流动安全。同时分类分级可为 API 敏感级别划分提供支撑，依据分类分级清单实现数据价值划分，为数据差异化管控提供依据。

敏感数据识别：根据敏感级别划分，动态制定敏感数据识别规则，通过规则分析自动识别未脱敏数据。

API 全盘发现：识别并建立 API 清单，对 API 进行可视化展现，发现 API 漏洞。

- 通过手动定义或 API 文件，建立 API 清单；
- 通过日志或流量分析，发现 API 清单未覆盖的请求；
- 对 API 活动做可视化展现；
- 结合威胁情报库，发现有漏洞的 API 应用服务器。

来源：上海观安信息技术股份有限公司

API 可视化管控：登记汇总各系统中注册，添加、登记的接口服务，实现对系统接口的汇总管理和可视化展示。

API 安全检测：API 安全检测是系统交互的屏障和保护伞，在接

口具体的使用过程中，通过提前预设告警规则、防御规则，记录非法操作、异常攻击等行为，匹配规则，实现防御阻断、告警，提高单个系统接口服务的有效性及保证整个生态系统的安全性、稳定性，为企业提供多重保障。

流量数据：通过协议解析，获取多系统接口行为记录，包括访问的接口、访问的 URL、源/目的 IP、源/目的端口、访问时间及流量等数据，为访问行为的安全审计、数据挖掘提供数据源。

审计告警：根据业务系统特点，对通过接口交互的敏感信息或关键字进行识别、告警设置，生成审计规则，对匹配规则的敏感信息进行相应操作，如区分日志类型（原始日志、重要日志、告警日志）、进行有效报警（邮件、短信）等，为系统接口交互行为审计提供及时预警及处理时间。

来源：上海观安信息技术股份有限公司

异常数据流动行为检测：从应用系统流量中提取用户访问行为的原始数据，计算相关的基础指标,构建数据模型进行机器学习和大数据分析，对数据访问建立行为基线，利用异常检测技术，从多个维度来识别异常数据访问行为，从而实现异常数据访问行为和数据泄露行为的感知和预警。

回溯取证：对接口业务行为进行完整的记录，并支持接口访问行为和事件回放取证。记录包括访问时间、访问者、访问凭据、访问请求参数、返回数据等。

API 数据安全态势分析：通过海量接口行为数据，运用 Hadoop 大数据支撑平台，快速大批量接口行为分析，辅助安全管理员提前预警阻断。

来源：上海观安信息技术股份有限公司

数据挖掘：对接口生命周期及接口的商业行为进行高效的梳理和分析，通过采用分类模型、预测模型、关联模型、聚类模型、异常值分析、协同过滤、文本挖掘等算法模型，为企业提供更优质的商业价值。

3. 实践应用

（1）背景

某运营商安全行为管控主要依赖传统的业务系统日志、4A 访问日志，数据来源单一，分析手段相互独立缺乏联动，缺少多维度分析；对接口调用异常、业务行为中敏感数据自识别监控、数据操作异常事件等新型事件，依赖现有传统审计方法无法有效识别和监测。

（2）应用

分析模块：分析业务流程包括数据采集、数据预处理、数据存储、分析引擎、结果输出等步骤。

风险场景模型：分析平台和业务场景的深度耦合，对系统业务风险点进行监测、控制，业务分析平台采用 2 套分析模型（机器行为模型、风险评分卡模型）对 4 大业务场景（接口风险告警、主机绕行告警、前台未授权查询信息、敏感数据操作监测）进行业务分析。

接口异常行为监测：基于流量探针对流量数据进行采集，根据接口小时段内容的接口类型、调用对象、访问时间间隔等数据维度构建特征工程，通过机器学习分类算法如随机森林，建立异常识别模型，从而通过模型识别出异常行为。

接口内容敏感识别：数据接口种类繁多，如何正确高效、识别敏感数据接口并进行行为分析，俨然成为工作难题。本次实践应用中通过流量探针，在下行流量数据中依赖命名实体识别、规则识别敏感数据，并对识别的敏感数据接口进行监控，精准管理敏感数据接口。

用户行为异常分析：关注用户对关键业务系统、敏感数据、敏感文件的操作行为，通过规则、基线等分析手段识别异常行为。

（3）成效

实践中完成 3 个业务风险场景建设，构建 2 套分析模型，日均处理 200G 数据，共监测识别异常事件 72 起、真实有效事件 67 起。

事件类型	事件数量
接口异常行为类	35
敏感数据范围异常	20
未授权查询用户信息	12

来源：上海观安信息技术股份有限公司

4. 发展趋势

当前，API 安全保护日渐成为网络应用的主要技术需求之一。人工智能和机械学习作为高效智能化的工具，已经被应用到了协议栈的各个层面上，以实现 API 的全栈安全防护。就下一步发展趋势来看，开发人员需要进一步加大对于 API 业务模型、分析能力、技术蓝图、以及合规性与标准化的深入研究与开发。API 安全实践的发展趋势包括：DNS 安全、安全设计、人工智能、机械学习驱动等。

（三）爱加密 API 安全实践

1. 安全方案

爱加密移动应用 API 安全防护方案秉持“分段保护，技术验证”的思路，在保障 APP 业务功能的前提下，对其调用或集成的 API 进行事前、事中、事后的全过程安全管理与防护。及时发现潜在的源码漏洞、破解盗用、异常调用等安全问题，并提供业务、数据、源码各层面的安全防护。

来源：北京智游网安科技有限公司（爱加密）

爱加密自动化安全扫描工具可针对 API 的源代码安全性、数据安全性与传输安全性等多方面进行检测，并对缺少源码保护、明文存储数据、非加密协议传输数据等问题进行重点侦测。

（1）源代码防护检测

源码反编译安全：检测 Java 文件是否进行加壳保护，未加壳可能面临被反编译的风险。

源码混淆检测：检测 API 源代码是否进行混淆处理，代码未进行混淆会在代码被反编译后导致核心代码可能被窃取，存在逆向代码还原到源码的风险。

so 文件保护检测：检测 so 文件是否为了实现不同软件之间的数据共享，设置内部文件为全局可读或全局可写，使得其他应用可以读取和修改该文件。

H5 代码安全检测：分析 API 中的 html5 文件是否经过混淆/加密操作。

密钥硬编码检测：检测 API 是否存在将加密算法密钥设定为固定值，导致不法分子可能通过反编译硬编码密钥破解接口加密机制情况。

（2）API 安全性检测

敏感信息获取检测：检测 API 中是否存在获取用户敏感信息的操作。

API 本地数据存储安全检测：检测 API 是否会将用户敏感数据明文存放在本地缓存目录，私有目录等。

日志数据安全检测：Log 日志是 APP 运行期间自身产生的，是对程序运行情况的记录和监控，通过 Log 日志可以详细了解 APP 内部的运行状况。

证书文件明文存储检测：查看 API 资源中是否包含明文的证书文件。

（3）API 数据传输检测

HTTP 协议检测：由于 HTTP 数据传输是明文传输的，导致 HTTP 数据容易被抓取、篡改，泄露用户密码等敏感数据，甚至通过中间人劫持将原有信息替换成恶意链接或恶意代码程序，以达到远程控制、恶意扣费等攻击意图。通过使用抓包工具在网络节点设置代理，侦听抓取 API 业务请求数据包，分析数据报文检查是否使用 http 协议传输数据。

业务接口漏洞测试：检查 API 是否存在与业务功能无关的服务器交互接口，通过侦听通信数据中的网络端口类型查看 API 是否存在可能的越权访问与脚本注入风险。

2.技术手段

自动化业务检测：将 API 恶意代码的行为特征具体化分析，创造行为自动化检测脚本，通过对真实运行环境的仿真模拟来诱导发现第三方 API 是否隐藏恶意行为与违规行为，将行为检测技术运用到检测方法当中，包括：

- 检测 API 读取隐私数据，如手机通讯录、通话记录、短信内容、IMEI、IMSI 等相关行为事件。
- 检测 API 完整的网络通讯事件，获取远程服务器 IP（包含地理区域）、端口号、域名、完整 URL。
- 检测 API 隐藏图标动作、执行系统高威胁设置等行为事件。
- 检测 API 运行过程隐蔽安装插件安装包行为事件。

➢ 检测 API 在运行生命周期内新建文件、编辑文件、删除文件等所有行为事件。

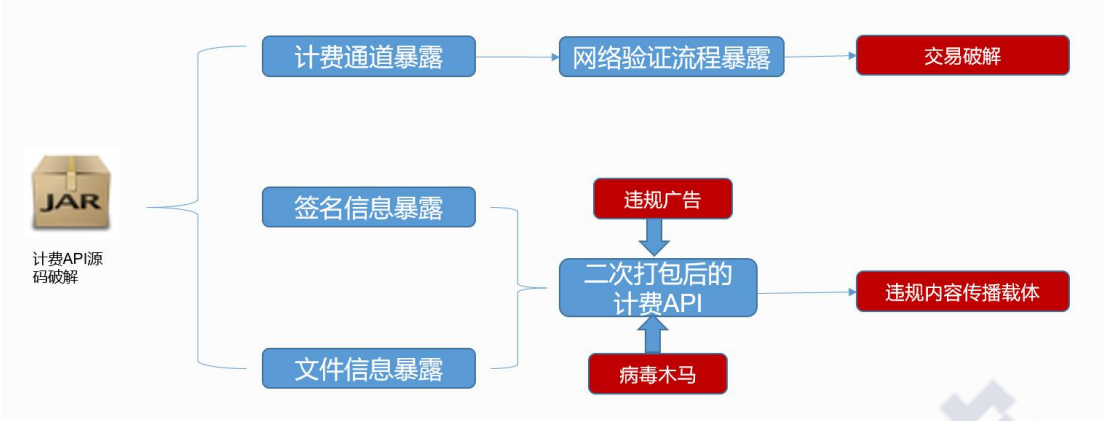
VMP 高强度代码加固：市面上普遍对 256 个 OpCode，进行了自定义指令替换，具体的操作数语法组合并不做处理。爱加密 VMP 对 OpCode 指令以及操作数都同时进行了指令转换处理，涉及操作数语法组合大概 541 种，在加密细粒度和强度方面具有显著优势。

API 探针技术：API 威胁感知可以进行自定义埋点探针数据采集，在后台对 APP 进行流程位置埋点探针，收集该埋点探针数据，在应用上线后埋点探针可进行远程操作，而后埋点下发。爱加密威胁感知系统支持多种响应形式的自定义下发，包括自定义弹窗，退出，提示，悬浮球，打开链接，启动应用，toast 提示，通知栏，预下载，下载并安装，跳转指定页面等。

3.实践应用

（1）运营商计费类 API 公开共享场景应用

某运营商开发自有计费 API 用于提供 App 内计费系统交易结算。由于缺少代码层面安全防护，API 接口遭到恶意破解，计费逻辑与关键文件被窃取，计费流程的完整性遭到破坏，导致交易破解与恶意计费事件发生。此外，遭破解的计费 API 可能被二次打包为携带违法广告、木马程序等内容的盗版 API，成为违法违规内容传播的载体。



来源：北京智游网安科技有限公司（爱加密）

爱加密通过技术手段对运营商计费类 API 进行源码保护，提高源码复杂度与完整性校验，防止被黑客破解分析，探知核心业务流程。同时对关键业务流程进行过程监控，对关键交易进行二次验证。

此应用场景下采取如下保护措施：

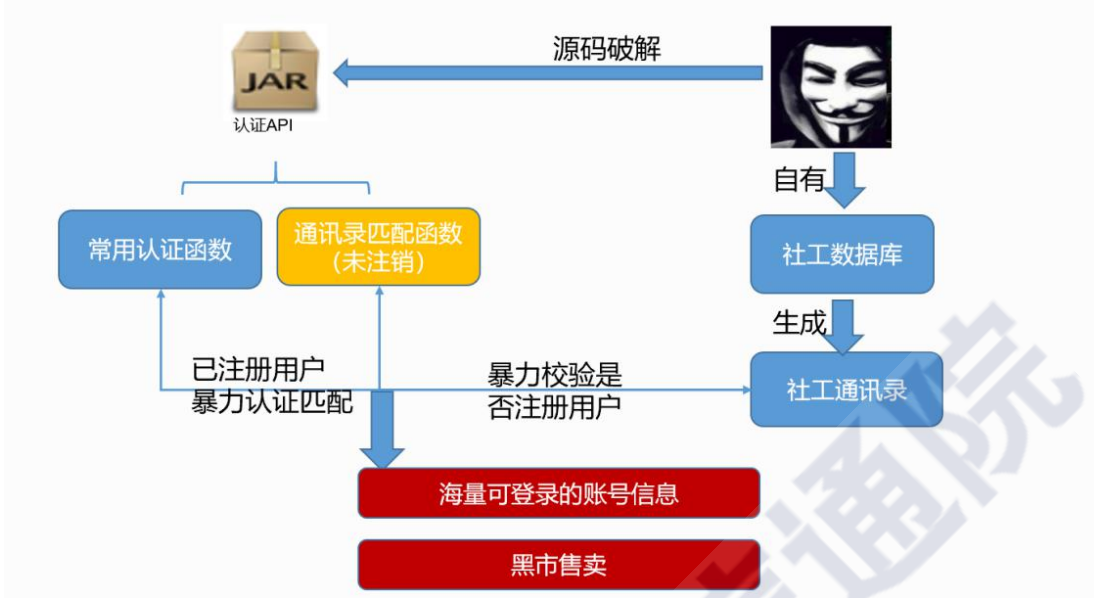
➢ 对 API 源代码进行加固处理，防止非法破解。API 加固保护包括对 jar 文件代码的虚拟化处理、so 库文件的安全防护等安全加固内容。同时防止 so 库被非法调用，对 App 的使用进行权限管理。

➢ 增加威胁感知探针，对 API 业务运行时的状态进行感知。在计费 API 运行时对关键核心步骤进行二次校验，对关键业务核心点进行完整性验证，出现的异常行为及时预警或阻断。

（2）互联网企业认证 API 对外开放场景应用

某互联网企业为推广业务吸引流量，向第三方开发企业与个人开放了自身 APP 的认证 API，实现便捷登录功能。由于未对 API 进行安全检测，被黑客通过 API 中的通讯录匹配功能暴力匹配用户姓名和密码，将海量黑产数据转化为有价值的用户账号数据在黑市兜售，

给企业带来极大的经济和社会信誉损失。



来源：北京智游网安科技有限公司（爱加密）

互联网企业在向社会公开自己的 API 时，需要对 API 做全面的安全检测，及时发现代码层面、数据层面与接口传输层面的安全漏洞，与 App 业务功能无关的接口应及时注销关闭，防止其被破解后形成潜在业务隐患。

此应用场景下采取如下保护措施：

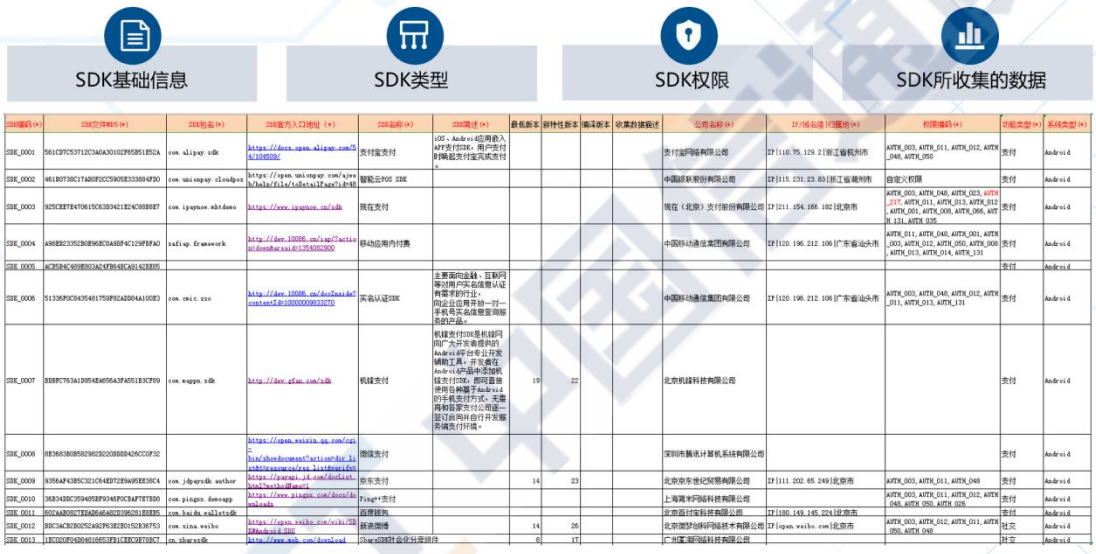
➢ 检测 API 源代码是否进行混淆，加固等安全技术处理。防止攻击者通过反编译工具得到 API 的代码后直接可读可定位等风险。

➢ 检测是否含有遗留日志数据，防止黑客通过 Log 日志详细了解 API 内部的运行流程。防止通过对日志搜索进行程序代码定位，从而找到 API 中关键代码进行分析修改。

➢ 增加威胁感知探针，对 API 运行时的业务请求频率进行监控。在出现高频率、涉及敏感数据的业务时向服务后台进行预警与客户端的防御响应。

4. 产品研发

目前 API 接口根据不同 APP 的开发场景被广泛集成到海量 SDK 中进行使用。爱加密结合其移动应用 SDK 领域安全积累，建立**移动 SDK/API 资产互联网监控平台**，通过大数据分析模型，提升相关风险预警的准确性和防护策略的有效性。



来源：北京智游网安科技有限公司（爱加密）

该平台依托于爱加密移动安全大数据平台的监管能力，针对数百万 APP 使用的 SDK/API 进行专向分类管理，当企业需要使用第三方 SDK/API 时，可通过爱加密安全大数据平台获取详细的状态与使用范围信息。

此外，平台提供针对企业自研 SDK/API 登记备案和管理功能，可对企业自研 SDK/API 是否遭违法违规调用进行快速查询和验证。平台提供的 API 全质量常态监测服务可对重大、突发安全漏洞实现第一时间检测与记录回馈，配合移动威胁感知系统的前端响应能力，

阻断风险扩散，精确划分影响范围，最大限度减小由于安全原因带来的负面影响。

中国信息通信研究院 安全研究所

地址：北京市海淀区花园北路 52 号

邮政编码：100191

联系电话：010-62308590　010-62308790

传真：010-62300264

网址：www.caict.ac.cn