



安全牛
AQNIU.COM

API安全技术应用指南

(2024版)

解密 API 安全之道 释放数据连接价值



安全牛
aqniu.com



版权声明

本报告为北京谷安天下科技有限公司（以下简称“本公司”）旗下媒体平台安全牛研究撰写，报告中所有文字、图片、表格均受有关商标和著作权的法律保护，部分文字和数据采集于公开信息，所有权为原著者所有。未经本公司书面许可，任何组织和个人不得以任何形式复制或传递本报告的全部或部分内容，不得将本报告内容作为诉讼、仲裁、传媒所引用之证明或依据，不得用于营利或用于未经允许的其他用途。任何未经授权使用本报告的相关商业行为都将违反《中华人民共和国著作权法》和其他法律法规以及有关国际公约的规定。未经授权或违法使用本报告内容者应承担其行为引起的一切后果 及法律责任，本公司将保留追究其法律责任的权利。

免责声明

本报告仅供本公司的客户使用。本公司不会因接收人收到本报告而视其为本公司的当然客户。任何非本公司发布的有关本报告的摘要或节选都不代表本报告正式完整的观点，一切须以本公司发布的本报告完整版本为准。

本报告中的行业数据主要为分析师市场调研、行业访谈及其他研究方法估算得来，仅供参考。因调研方法及样本、调查资料收集范围等的限制，本报告中的数据仅服务于当前报告。本公司以勤勉的态度、专业的研究方法，使用合法合规的信息，独立、客观地出具本报告，但不保证数据的准确性和完整性，本公司不对本报告的数据和观点承担任何法律责任。同时，本公司不保证本报告中的观点或陈述不会发生任何变更。在不同时期，本公司可发出与本报告所载资料、意见及推测不一致的报告。

在任何情况下，本报告中的信息或所表述的意见并不构成对任何人的行为建议，也没有考虑到个别客户特殊的目的或需求。客户应考虑本报告中的任何意见是否符合其特定状况，若有必要应寻求专家意见。任何出现在本报告中的包括但不限于评论、预测、图表、指标、指标、理论、陈述均为市场和客户提供基本参考，您须对您自主决定的行为负责。本公司不对因本报告资料全部或部分内容产生的，或因依赖本报告而引致的任何损失承担任何责任，不对任何因本报告提供的资料不充分、不完整或未能提供特定资料产生的任何损失承担任何责任。

目 录

第一章 API 安全概述 7

1.1 API 的发展背景	7
1.2 API 面临的安全挑战	8
1.3 API 的安全理念	10
1.4 国内外相关政策及标准	11

第二章 API 安全技术 16

2.1 API 安全框架	16
2.2 核心能力简介	18

第三章 应用现状及场景化分析 23

3.1 API 安全需求及应用现状调研	23
3.2 API 安全的典型应用场景分析	32

第四章 API 安全建设指南 37

4.1 建设挑战	37
4.2 基本建设原则	38
4.3 方案选择建议	40
4.4 年度代表性供应商介绍	42

第五章 案例研究 63

5.1 车联网公有云环境的 API 风险监测能力建设案例	63
5.2 API 安全管控系统助力电信行业网络防护的案例	67

5.3 金融行业云原生 API 安全体系建设案例	70
5.4 API 安全监测系统助力医疗企业数据安全防护的案例	73
5.5 移动应用环境的 API 安全能力建设案例	77

第六章 新兴技术对 API 安全的影响 81

6.1 零信任技术	81
6.2 人工智能（AI）和机器学习（ML）	82
6.3 大数据技术	82
6.4 云计算和容器化技术	82

参考资料 84

引言

API 是软件集成、系统集成、远程服务访问的基础。随着模块化、面向对象及微服务开发的进一步应用，API 从系统内部连接逐渐扩展到系统外部，并在整个互联网范围内连接起相互独立的各个业务节点，人与服务、服务与服务、系统与服务之间的信息交换都在 API 的基础上进行着。随着 SaaS 化和云服务的兴起，基于 API 的软件集成已成为构建现代应用程序的关键方法。开发者基于 API 构建应用、开放能力、共享服务，形成了以 API 提供者、消费者为主的 API 生态经济。

然而，API 自身的安全性，如不安全的协议框架、开发缺陷和漏洞，不仅给应用程序和 Web 应用带来严重的安全隐患，还因为大量 API 的外部暴露，极大地增加了业务系统和数据的攻击面，为不法分子提供了可乘之机。在日趋严峻的网络安全形势下，赏金猎人和针对 API 的自动化攻击工具使 API 自身的缺陷更容易被发现和利用。这些漏洞可能导致非法访问、数据泄露、SQL 注入和跨站脚本攻击等一系列安全风险，给企业造成系统破坏、业务中断和经济损失。

API 作为应用软件的重要组成部分，也是软件安全、业务安全和数据安全的底层基石，是国家网络安全和数字经济发展的重要前提。为保障国家数字经济的长效建设，行业监管部门在贯彻网络安全的基础上进一步着手 API 安全治理，陆续出台应用程序接口安全相关的细则，包括《应用程序接口规范》《云应用安全技术标准》《数据安全技术数据接口安全风险监测方法》等等。这些规范分别从评估、审计、漏洞检查、隐私敏感权限等维度提出了具体要求。

为在网络安全建设中帮助用户更好地开展安全规划、API 安全建设，并给用户提供有效的 API 安全框架、产品方案、厂商支持，安全牛即日起正式启动《**API 安全技术应用指南（2024 版）**》报告（以下简称“报告”）研究工作。报告基于调研对 API 的安全风险进行识别，从 API 安全测试、风险可见性、API 风险防护等多方面对 API 的安全能力建设提出建议；同时，基于调研也对厂商的 API 安全产品或解决方案进行能力评估，并对该领域的年度代表性厂商进行能力评估、方案推荐和落地应用案例展示。为用户选择合适的产品和厂商提供有效参考。

报告关键发现

- 调研显示，当前企业对 API 漏洞利用、数据安全问题最为敏感。但，大多数用户认为 API 风险对企业的影响程度为中低水平，API 风险影响还相对有限。反映企业对 API 风险有一定认识，但重视程度还不高。
- 调研显示，企业通常会遭受多种类型的 API 攻击事件，而 API 的敏感数据、身份验证是最容易遭受攻击的两个薄弱环节。
- 调研发现，几乎所有类型 API 安全产品都在 API 资产识别功能中提供了数据资产识别及数据分类标识功能。这预示着，API 安全将有可能会成为数据流转合规的一项标准化管理手段。
- 调研显示，在 API 安全建设中检测、监测和防护类产品均有涉及，并且半数以上企业采用了两种以上类型的工具。其中，API 网关和 API 安全监测平台被认为是最有效果的两个产品类型。
- API 安全建设方面，调研显示，大多数企业的 API 安全建设并未提到日程上，观望者较多，整体预算分布也偏于保守。
- API 作为一个新兴赛道，厂商的参与度较高，这些能力提供者来源于多个传统领域。其中，应用安全和业务安全厂商占比最高（占比 35%）；数据安全和网络安全厂商次之（占比各 18%）；同时，专注于该赛道的新兴厂商也较多（占比约 30%）。从提供的 API 安全方案类型看，主要有访问控制网关类、风险监测防护类和数据流转管控类三种典型类型。其中，提供风险监测类方案的厂商最多。
- 目前阶段，尽管市场上 API 安全方案不断地推陈出新，但 API 安全的应用模式仍处于探索阶段。建设中，识别、检测、防护等核心能力存在不同程度的技术挑战，风险处置的自动化能力也尚显不足。
- 从 API 安全技术成熟度演进的视角来看，安全牛认为零信任、人工智能、大数据，以及云计算四类新兴技术将能有效赋能 API 安全，在提升 API 风险检测精准度、覆盖度和自动化防护处置能力方面提供显著助力。

第一章 API 安全概述

1.1 API 的发展背景

API (Application Programming Interface, 应用程序编程接口) 是一组代码逻辑的抽象，它通过某一种特定的函数关系对功能源码进行封装，使其成为可被外部系统集成和重复调用的组件。API 可以实现代码共享、提高系统兼容性和应用软件开发效率，具有很强的连接力，是代码开发过程中不同功能模块之间信息交换的重要纽带。

模块化、面向对象和微服务等现代软件开发模式的广泛应用，将人与服务、设备与服务、服务与服务之间的信息交互都加载到了 API 接口上。API 成为现代应用软件构建的关键方法。随着互联网、物联网、移动互联网的发展，API 的应用场景从本地扩展到 WEB 应用、移动应用、云原生及 AI 等更广泛的应用领域，API 的使用方法也从进程内部调用逐渐扩展到远程调用。在 SaaS 化和云服务市场进一步推进下，远程访问、远程办公和云服务常态化，API 的应用持续外化。大量商业化的容器、微服务开始出现，开发者基于 API 构建应用、开放能力和共享服务，形成了以 API 提供者和消费者为核心 API 经济市场。



图 1 API 应用的演进过程

然而，API 自身的安全缺陷，不安全的协议框架，开发缺陷和漏洞，都随着服务的广泛调用一览无余地暴露到了互联网，这不仅使应用程序和 Web 应用面临严重的安全威胁，还因为大量 API 外部暴露，极大地增加了业务系统和数据的暴露面，为非法分子提供了可乘之机。给企业网络和业务系统安全埋入了不同程度的安全隐患。

1.2 API 面临的安全挑战

早期 API 安全主要侧重于开发阶段 API 的安全性，典型方式是写入技术标准中的操作规范，如 OPEN API。它通过一致性的 API 描述来提高 API 可用性，同时也提出一些规范性的遵循措施来规避工程师经验缺少和错误操作问题，避免个人身份等敏感信息的路径或查询参数主动暴露在客户端或服务器日志中。

随着全球的数字经济转型，企业东西向、南北向的连接需求进一步扩大，API 的暴露面、开发缺陷、漏洞产生攻击面都随之扩大。随着 API 承载数据价值的进一步提升，外部的赏金猎人、自动化攻击工具、渗透攻击、供应链攻击等针对 API 的复杂攻击日益加剧。API 的漏洞利用变得更加容易，API 面临的安全挑战也日益严峻。

(1) API 与应用软件一样拥有先天性缺陷和脆弱性风险

API 也是一类代码，跟源码一样拥有先天的缺陷和脆弱性。OWASP 作为应用软件安全研究的公益性组织，2019 年首次提出 API 十大安全风险。API 面临的安全风险。其中，授权失效、身份验证失效、数据暴露问题是严重级别最高的三类 API 风险。但 4 年之后，在 2023 年版的 API TOP10 风险报告中显示，API 授权失效、身份验证失效等风险仍然高居不下。



图 2 OWASP API TOP10 风险

在 NVD 漏洞库中以“API”为关键字进行检索，近 3 个月有 300 多条 API 直接相关的漏洞。这些漏洞被利用后会导致中间人劫持、API 攻击、恶意代码入侵、隐私信息泄漏、远程代码执行（RCE）、勒索等严重的网络安全事件。

根据 Gartner 相关研究，2022 年，超过 90% 的 Web 应用程序遭受的攻击都来自 API 而非界面。对照近些年发生的 API 安全事件，能进一步感受到 API 风险态势的严重性：

- 2022 年 5 月，CVE-2022-1388 F5 BIG-IP iControl REST 身份认证绕过漏洞，导致授权访问机制失效；

- 2021 年 11 月，Apache 开源项目 Log4j 漏洞，由于在 JNDI 接口 lookup 查询时可以注入恶意 payload，造成远程代码执行（RCE），使全球的 Apache 用户受到影响；
- GraphQL API 漏洞（2020-7 API5- 失效的功能级授权），API KEY 泄露（2020-2 API2- 失效的用户身份认证），Facebook OAuth 漏洞（2019-12 API5- 失效的功能授权）、Paypal 委托授权漏洞（2019-7 API1- 失效的对象级授权）、Hadoop 管理 API 漏洞（API5- 失效的功能级授权 2018-6）等。

(2) API 数量持续增长不断扩大企业的攻击面

今天所有应用软件、业务系统以及网络基础设施都是在 API 连接的基础上建立起来的。随着业务云化、远程办公常态化，API 又成为企业网络、业务系统面向互联网访问的直接触点。内外部的 API 数量随着企业业务的持续增加，都在快速增长。大量暴露在外的 API 成为黑客实施攻击重要的突破口；同时，系统内部的 API 也为攻击者进一步横向渗透提供了重要渠道。API 天生的缺陷加上后天的暴露面，成为企业网络和业务系统最薄弱的环节之一。

(3) API 访问通常要穿透网络边界 成为不被企业保护的资产

据国家 CNVD 漏洞共享平台分析：80% 以上的漏洞都属于可被利用来实施远程网络攻击的类型，而远程访问攻击大多都与 API 接口的身份验证绕过、授权管理失效、数据出栈入栈的访问管理有关。然而，传统的访问控制设备通常缺少针对 API 接口的安全策略，这使企业边界防护常常失效，API 成为不被企业保护的资产。企业部系统也面临着唇亡齿寒的窘境。

(4) API 数据安全流通对企业数据安全合规提出了新挑战

为保障数据经济健康发展，国家发布了数据安全法和个人信息安全法，从数据全生命周期安全和个人隐私信息安全方面提出了严格的合规性要求。随着数据要素和流转政策进一步开放，数据流转管控也被提上一个新高度。特别是，国家“数据二十条”的发布，要求加强数据流转过程中的数据要素治理。API 作为数据共享和交换的重要载体，承载了大量的敏感数据和个人隐私信息，肩负了数据安全流转的重任。API 数据安全流通的要求对企业数据安全合规也提出了新的挑战。

(5) API 资产管理缺失 安全状态和安全风险不可见

API 不仅随着业务需求数量快速增长，还会随业务变化和软件更新动态变化。长期的业务调整和软件更新，导致系统内部暗藏未关闭的过时 API、僵尸 API。由于 API 资产管理缺失，API 的健康状态、安全状态不可见，这些遗忘的 API 缺少维护和更新，容易沦为黑客攻击利用的工具。API 资产管理的缺失与其内生的脆弱性以及应用环境的复杂性耦合在一起，进一步增加了企业的安全风险。

● API 安全概述

数字化转型中，API 与互联网应用、移动应用、物联网应用、云计算应用息息相关，API 安全是企业业务及应用系统安全的重要前提。

1.3 API 的安全理念

API 风险不仅直接关系到用户数据、企业业务、应用系统安全，还直接影响到国家数据安全，导致企业违法并被监管部门处罚，因此迅速引起了社会各组织机构的高度关注。目前，国内外的企业，从应用软件开发商到安全厂商、第三方研究机构都开启了 API 安全理念的探索，涉及内生安全、攻击防护、访问管理、全生命周期管理多个方面。代表性的 API 安全理念，包括：Forrester 认为解决 API 安全问题需要关注 API 全生命周期管理，并从治理、发现、测试、认证与授权、防护、攻击检测、响应、代理访问八个方面采取安全措施。

- Gartner 认为保护企业内部和外部的 API 免受漏洞利用、滥用、访问违规和拒绝服务（DoS）攻击的一种安全策略。包括 API 资产可见性、API 安全测试、API 威胁保护等多个方面。
- BM 认为 API 安全是指保护应用程序编程接口（API）免遭滥用、恶意机器人攻击和其他网络安全威胁的实践和程序。
- Forrester、Gartner、IBM 分别从过程管理、漏洞利用、攻击防护角度阐述了 API 安全的理念。

API 是应用构建的一种重要方式，是应用软件不可分割的一个组成部分。在 API 面临的复杂的安全挑战下，安全牛认为：**API 安全理念应从 API 安全防护向 API 安全治理演进，遵循应用软件安全管理原则，覆盖 API 生产到使命结束的全生命周期。**

具体地，API 安全是指 API 在生产、部署、运营阶段所实施的一系列安全管理活动，包括规范 API 的使用行为，实施安全运行策略，采取风险监测、防护、响应等风险闭环措施等等。其目标是减少应用系统构建过程中形成的 API 攻击面，保护 API 协议、结构免受外部攻击，保障 API 承载的数据、应用和业务安全运行。

基于 API 全生命周期，报告从 API 开发、部署和运营三个环节，进行 API 安全分析。以下分别将三个阶段对应的安全建设称作安全开发、安全部署和安全运营。

- **安全开发** 指在 API 开发阶段，遵循安全开发规划，对代码进行安全开发、安全测试、构建，并进行 API 接口文档化、代码维护的工作。由于 API 发布的灵活性，API 开发非常符合 DevOps。DevSecOps 在敏捷开发模式下可以为 API 安全提供很好的助力。
- **安全部署** 指为保证 API 被正常访问和使用，在 API 上线发布过程中，采用安全部署、安全配置，并对 API 的变更、下线进行维护管理的工作。关注 API 自身的可用性、完整性和机密性。

- **安全运营** 指为保障业务系统的安全性，在业务运营过程中，进行 API 资产管理、风险监测及风险防护处置工作。侧重业务系统整体的安全管理和风险控制，降低业务安全风险。

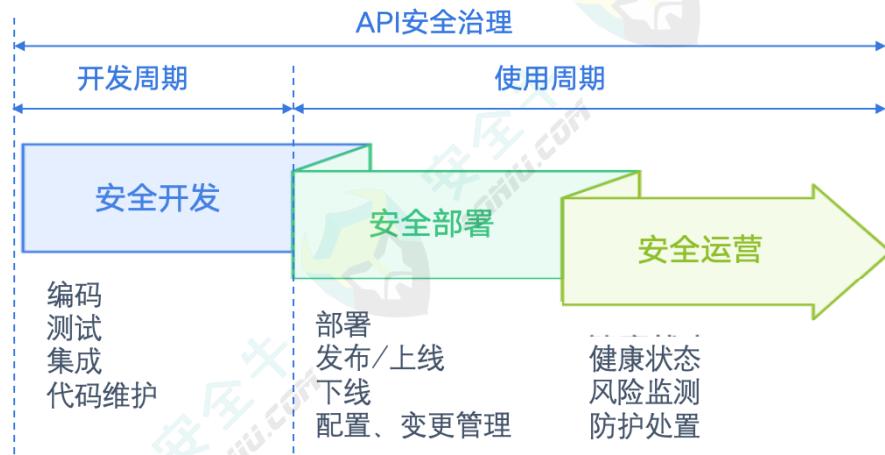


图 3 API 安全治理全生命周期

1.4 国内外相关政策及标准

政策上，国内外都很少针对 API 安全直接出台政策和法规，但多数国家和组织的通用安全法规和行业安全法规中都有提到 API 的安全要求并监管企业执行和遵守。随着数据泄露和隐私问题的日益增多，组织也必须确保其 API 符合法规和标准要求。因此，行业规范和法规遵从性仍是当前 API 安全市场最主要的驱动力。

1.4.1 欧盟

欧盟在 API 安全方面最有影响力的法规是 GDPR 和 NIS 指令。这两部法规分别从个人数据和隐私安全方面对 API 安全提出了相应要求，并对通过 API 访问和共享数据的方式实施严格的控制。这些法规倒逼数据服务商在 API 设计和实现过程中充分考虑数据保护和隐私要求，建立 API 治理框架来管理和保护 API 从设计到部署的整个生态过程。API 服务提供商也开始完善 API Guide。

(一) 《通用数据保护条例》(GDPR)

GDPR 是一项全面的数据保护和隐私法规，旨在加强整个欧盟 / 欧洲经济区的个人数据的保护和控制。该法规也是欧盟 API 安全方面的最重要的法规之一。

该法规 2018 年 5 月生效。之后各成员国陆续出台了《GDPR 个人数据安全指南》帮助企业遵从 GDPR 合规。加强 API 治理是 GDPR 指南的重要手段之一。指南建议企业从 API 设计、发布、API 隐私数据传输加密、访问验证、最小化授权、风险监测和响应等方面加强 API 管理。具体规避措施包括：

● API 安全概述

- 发布 API 之前，检查对 OWASP TOP10 风险的抵抗力；
- 遵从指南中 API 数据共享安全的建议；
- API 的实施必须符合标准的安全措施，如适当的认证机制，对授权定期管理或加密通信手段；
- 应提供一个 API 沙箱，以便通过虚构数据验证和测试风险影响。

(二) 网络和信息安全指令 (NIS)

网络和信息安全指令 (NIS Directive) 是欧盟为提升成员国网络与信息系统的安全性而制定的一项重要法规。该指令于 2016 年 8 月生效，并要求各成员国在 2018 年 5 月前将其转化为国家法律。

NIS 指令的更新版 NIS2 于 2024 年 10 月生效，新指令的范围将扩大到包括更多关键基础设施和数字服务，涵盖了直接影响 API 安全的广泛网络安全要求，这将对 API 安全产生更直接的影响。组织必须通过实施更有针对性的身份验证、加密、监控和事件响应措施来确保企业的 API 安全。遵守 NIS2 涉及将这些实践整合到整体风险管理和服务策略中，确保 API 作为 IT 基础设施的一部分受到网络安全威胁的保护。

此外，《修订支付服务指令 (PSD2)》等开放银行法规也要求金融企业的 API 支持安全、标准化的数据共享方法，并确保使用的 API 符合软件成分分析 (SCA) 的透明度要求。

1.4.2 美国

美国 API 安全相关的政策，一方面是在发布时间较早、对数据隐私安全要求较高行业法规及其标准中，典型的有 HIPAA（健康保险便携性和责任法案）、PCI-SSC（支付卡行业安全标准委员会）、21 世纪治愈法案。这些法规和标准对医疗、金融等敏感行业的数据隐私安全提出了严格要求，而 API 作为这些行业数据共享和集成的重要方式，必须符合相应的安全规定。

另一方面，体现于美国最近陆续发布的新政策中。在美国的新政策趋势方面，2024 年 4 月，美国众议院和参议院讨论并发布了《美国隐私权法案》草案，10 月 30 日美联邦政府又推出了《联邦零信任数据安全指南》，强调以数据为中心的安全防护，通过零信任架构和核心能力提高联邦机构系统的安全韧性。这些新政，分别从法规要求和技术指南方面加速完善美国国家层面敏感数据、隐私的安全要求和防护能力。API 作为承载敏感数据的重要载体，这一趋势也必会进一步促进 API 安全实施。

(一) 隐私权法案

《加州隐私权法案》(CCPA) 是加利福尼亚州于 2018 年通过的一项重要隐私保护法律，旨在保护加州居民的个人可识别信息 (PII)。该法案在 2020 年经过进一步完善，通过了新的《加州隐私权法案》(CPRA)，新法案增加了更多针对加州居民的隐私权利，并由加州隐私保护局负责实施和执行。CPRA 进一步扩展了消费

者的权利，包括纠正不准确信息的权利、选择退出自动决策的权利以及限制敏感个人信息使用的权利。

2024 年 4 月，美国众议院和参议院对《美国隐私权法案》草案进行了讨论并发布了该草案。旨在加强数据保护和隐私权利。该法案的实施后将会统一美国的数据隐私权，进一步扩大 API 安全管理的范围。

(二) HIPAA

《健康保险流通与责任法案》(HIPAA) 是美国 1996 年发布的联邦法律，旨在保护患者的健康信息，并确保数据安全。HIPAA 对 API 安全的要求涵盖了访问控制、审计控制、传输安全、加密、风险管理、数据完整性以及身份验证等多个方面，以确保健康信息 (PHI) 在 API 使用过程中的安全性和合规性。

按该法案要求，处理受保护健康信息的 API 必须使用加密、安全访问控制和审计日志来遵守 HIPAA。

(三) PCI 安全标准委员会 (PCI-SSC)

PCI 安全标准委员会 (PCI Security Standards Council, 简称 PCI SSC) 是一个联盟性的组织，旨在制定、维护和推广 PCI DSS 标准（支付卡行业数据安全标准），旨在保护信用卡和借记卡交易中的持卡人数据安全。Cloud SIG 是该组织中专注于云计算领域的支付卡安全问题的特别小组，2018 年 4 月该小组发布了与云环境相关的 PCI DSS 补充指南《PCI SSC Cloud Computing Guidelines》为如何在云环境中维护支付卡数据安全提供指导。该文件提出软件接口和 API 安全的注意事项，并要求企业在使用提供商暴露的 API 时，要确保满足所有适用的 PCI DSS 职责。

- APIs 和其他公共接口的设计应防止意外滥用和恶意绕过安全控制，弹性身份验证和访问控制、强加密和实时监控是保护这些接口的控制措施的例子；
- 所有影响持卡人数据和持卡人数据环境的 API 调用必须按照其 Appendix A Req10 的要求进行记录和审查。或者，当调用传输持卡人数据的 web 服务调用时，它应该通过加密隧道（例如 SOAP 本机加密或 TLS 隧道）。

(四) 《21 世纪治愈法案》

《21 世纪治愈法案》(21st Century Cures Act) 是美国国会于 2016 年 12 月通过的一项重要立法，由前总统奥巴马签署生效。旨在推动医疗信息技术的互操作性，同时确保患者数据的安全性和隐私保护。具体包括：

- 采用标准化的 API 方式；
- API 在传输数据时必须使用安全的协议；
- API 开发者必须持续维护 API 的安全性和功能性等等。

● API 安全概述

(五) API 安全性测试标准

标准支撑方面，漏洞、风险管理方面标准在 API 安全性的测试及测试 API 安全性方面给出了指导方针和最佳实践，有助于识别和解决 API 相关安全风险。

- **ISO/IEC 29147**: 是漏洞披露的国际标准，包括对 API 进行安全测试和报告漏洞的指导方针。
- **NIST SP 800-53**: 是美国国家标准与技术研究院（NIST）发布的标准，为信息安全和风险管理提供指导方针，包括 API 的安全测试。
- **NIST SP 800-115**: 是进行渗透测试的指南，其中包括测试 API 的具体指南。
- **OpenAPI 规范 (OAS) 3.0**: 这是定义和记录 API 的标准，包括安全测试和漏洞管理的指南。
- **OWASP API 安全测试项目**: OWASP API 安全测试项目是测试 API 安全性的综合指南，包括详细的测试过程和检查表。

1.4.3 澳大利亚

澳大利亚随着政府服务的现代化，越来越多地依赖数字平台和方法，但其解决方案的连接性、服务互操作性和数据安全性方面出现了新的挑战。为了应对数字化带来的挑战，澳大利亚政府面向 API 开发者发布了《应用程序编程接口（API）设计标准》旨在确保 API 的安全性、稳定性和易用性。内容包括 API 设计的基本原则、安全措施、传输安全、认证与授权、受信任的数字身份框架、速率限制、错误处理、审计日志、输入验证、内容类型验证、网关安全特性以及保护标记等诸多方面。

标准强调所有传输必须通过 HTTPS 进行，使用至少 TLS 1.2 版本，并且所有证书必须来自 SHA-2 加密哈希函数，最小密钥长度为 2048 位。在认证与授权方面，推荐使用 Authorization: Bearer 头进行认证 / 授权，例如使用 JWT 令牌，并建议提供刷新令牌以延长现有令牌的过期时间。

此外，该政府还建议最好使用 WoG API Gateway 平台中可用的安全策略，而不是应用后端的 API 安全策略。

1.4.4 中国

中国是典型的垂直立法的国家。《中华人民共和国网络安全法》作为我们国家网络安全的基本法，从个人信息安全角度为 API 安全确立了基本目标。细分领域，《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》进一步从数据采集、共享、隐私信息保护及违规责任方面提出了 API 安全要求；《App 违法违规收集使用个人信息行为认定方法》，也从市场监管方面对 APP 违规收集个人信息行为进行了判定。这些政策，不仅在 API 在设计和使用过程中进行了合规性要求，也为 API 安全监测和验证提供了依据。

国家和行业机构也先后出台了国家标准、行业标准，从技术方面为落实 API 安全提供了参考。

- JR/T 0185-2020《商业银行应用程序接口安全管理规范》是由中国人民银行发布的一项金融行业标准，旨在加强商业银行应用程序接口的安全管理，2020 年 2 月 13 日发布并实施。该规范详细规定了商业银行应用程序接口的类型与安全级别、安全设计、安全部署、安全集成、安全运维、服务终止与系统下线、安全管理等要求，适用于银行业金融机构、集成接口服务的应用方以及第三方安全评估机构。
- GB/T 35273-2020《信息安全技术 个人信息安全规范》是国家标准委发布，“网安标委”负责管理的一项国家标准，旨在规范个人信息的处理活动，确保个人信息的安全，2020 年 10 月正式实施。该标准明确了 API 开发与个人信息安全的结合要求，包括嵌入第三方插件（SDK、API 接口）、接入第三方服务的相关措施。
- YD/T 4248-2023《电信网和互联网应用程序接口数据安全技术要求和测试方法》是一项由工业和信息化部主管的标准，旨在规定电信网和互联网应用程序接口（API）的数据安全技术要求，并提供相应的测试方法和判定准则。该标准 2023 年 8 月 1 日正式实施。
- 2024 年 8 月 2 日，国家“网安标委”发布了国家标准《数据安全技术 数据接口安全风险监测方法》征求意见稿，旨在为各类组织提供数据接口安全风险监测的指导。该标准详细阐述了数据接口安全风险监测的方法、内容和流程，明确了监测各阶段的要点，并定义了数据接口及其要素关系。

第二章 API 安全技术

2.1 API 安全框架

为给 API 安全建设提供指导，报告基于研究从安全治理的视角，遵循“安全左移 持续运营”和“体系化建设”的原则，围绕开发、运行和运营三个环节进行 API 全生命周期安全能力构建。

如图 4 所示。API 安全框架以安全运营为目标，以事前、事中、事后的响应处置为手段实现 API 全生命周期的风险闭环管理。系统框图对应开发、部署和运营三个阶段的安全能力，涉及开发安全、访问控制、风险识别、风险监测、风险防护、安全审计 6 个核心组件。

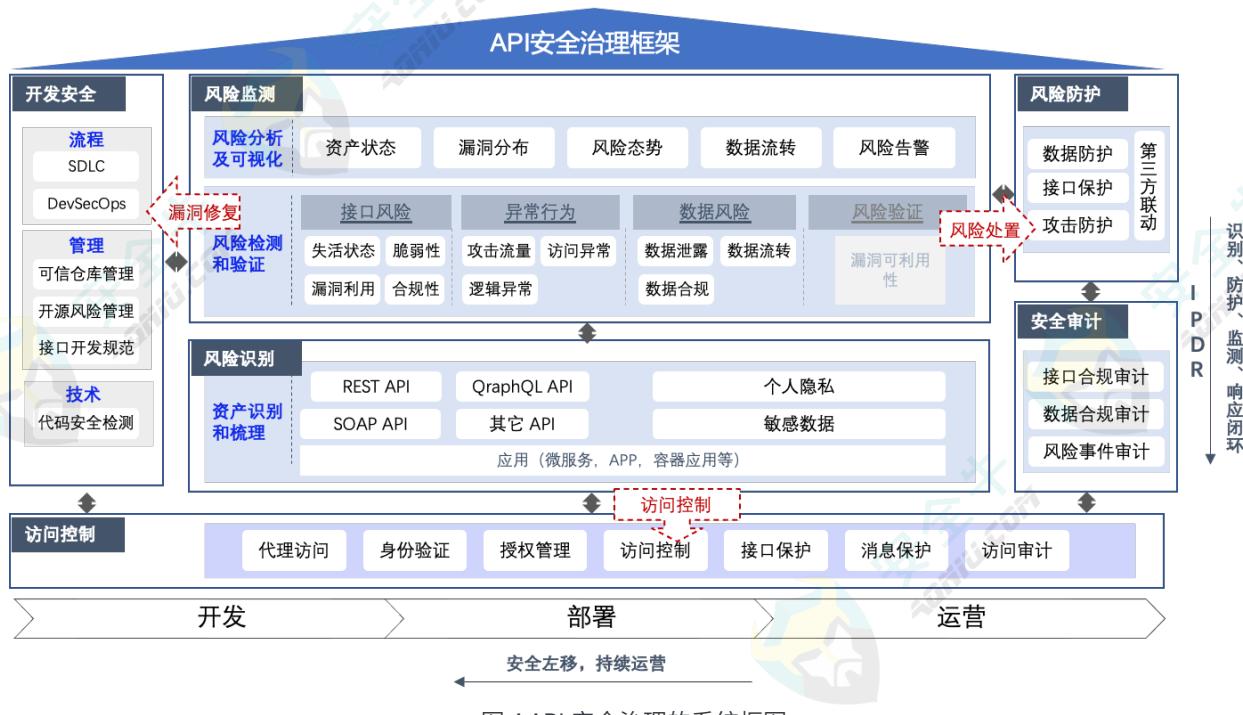


图 4 API 安全治理的系统框图

其中，开发安全对应开发阶段的安全风险；访问控制是 API 上线部署阶段的安全能力；风险识别、风险监测、风险防护、安全审计应对 API 运营阶段的安全能力。以下从安全开发、安全部署和安全运营三个分别阐述 API 的安全能力。

(1) 安全开发

安全开发 是保障开发阶段安全的一个重要手段。API 的安全开发适用于软件开发和软件供应链安全管理的原则，包括遵循安全开发设计流程、API 安全开发规范，采用代码安全的技术和手段做好第三方服务和 SDK 接口的可信管理，应用安全测试工具保障 API 对应源码满足基本的安全合规要求，减少代码自身的漏洞和脆弱性。

(2) 安全部署

安全部署 是为保障 API 所提供服务的稳定性和合规性，在 API 部署、发布、运行维护过程中实施访问控制策略，并维护上线 API 的配置管理的过程。访问控制策略是保障 API 安全运行的基础，具有较强的确定性，多数可以直接用于访问控制，包括：代理访问、身份认证、授权管理、访问控制、数据安全合规（加密、脱敏）、访问审计、接口保护（限速、限流、防止恶意调用等）等。API 上线后的配置管理是减少僵尸 API、影子 API 的主要手段。

(3) 安全运营

安全运营 指为应对各类针对 API 的攻击风险，保障 API 调用数据的合规性和业务逻辑的安全性，减少 API 攻击对业务的影响，对 API 进行风险监测和风险应对的过程。安全运营应遵循 IPDR “识别、防护、检测、响应” 风险闭环管理的原则，由资产识别、风险检测、风险分析和可视化、风险防护和风险审计 5 个能力组成。

- API 资产识别 是 API 风险检测的基础。为全面地识别 API 风险，API 资产识别通常不仅包括 API 接口本身，还要包括承载 API 接口的应用以及 API 接口上所承载的数据。为方便对 API 资产监管，API 资产识别阶段还要对资产标识，特别是按承载业务数据的敏感程度进行分类分级。
- API 风险检测和验证 风险检测指识别风险并进行告警，是 API 风险分析可视化的重要前提。API 风险类型复杂，涉及 API 自身脆弱性和漏洞利用风险、行为风险、API 数据风险多个方面，需要不同的风险检测引擎。因此，风险检测层的工作通常是检测到风险后，向分析平台告警。由分析平台进一步分析后进行响应和处置。
- API 风险分析和可视化 风险分析可视化指结合告警、情报、业务环境，对风险告警进行综合地关联分析，并对风险态势进行展示、管理和响应。风险分析通常需结合多方面的情报数据进行关联分析确认风险的真实性，特别是在发现漏洞风险时，对漏洞存在的真实性也要进一步结合漏洞验证进行确认。
- API 风险防护 由于 API 风险类型的复杂化，API 安全需要多层次、多维度的风险防护能力，包括攻击防护能力、数据防护能力、访问控制防护能力等，对于确定的 API 漏洞要采取漏洞补丁或进一步回归到开发侧进行修复。为提高风险管理处置的效率，API 风险处置需要采用系统化、联动防御方式，结合企业的安全建设、安全运营能力，形成多层次防御、纵深联动的一体化安全运营。
- API 安全审计 安全审计是将 API 纳入常态化安全管理，并保证 API 安全管理持续有效的一种重要方式。这包括 API 资产审查、访问控制合规审计、API 数据安全审计、风险审计等多维度，涉及日志记录、事件溯源、合规性检查、报告输出、数据合规检查等技术手段。

从根本上缓解 API 的安全隐患和数据调用风险，实现全面 API 安全治理。API 风险监测要与开发系统、

● API 安全技术

运行系统、防护系统之间建立有效的问题反馈通道和协同机制，通过安全运营能力分别应对 API 运营中的合规类缺陷、攻击风险、漏洞缺陷，实现 API 安全持续运营。如，将合规缺失的策略应用到访问控制系统，API 风险纳入风险防护体系，将漏洞利用问题回归到开发侧验证和修复。



图 5 API 安全持续运营

2.2 核心能力简介

API 的核心能力，包括：开发安全、访问控制技术、风险分析和可视化、资产识别、风险检测、风险防护、风险响应七个核心能力。这些都是确保 API 全生命周期安全的重要技术。



图 6 API 安全建设的核心能力

2.2.1 API 访问控制

API 拥有主 - 客体网络访问属性，需要应对各类访问风险，访问控制是 API 的第一道安全网关，也是 API 合规性的基础安全策略。

API 访问控制策略是基于 API 调用和访问过程中的安全风险，而向 API 接口和 API 数据实施的基于身份、规则匹配类安全策略。包括：身份认证（Authentication）、授权管理（Authorization）、账号访问控制（Accounting）、访问审计（Auditing）、接口保护（接口限速、限流、防止恶意调用、数据加密、脱敏等）、数据合规保护（加密、脱敏）。

API 访问控制继承了传统 3A、4A 访问控制的基本原则，告警的准确度较高，可直接应用阻断、放行等处置策略。随着零信任理念的广泛应用，API 的访问控制在规则策略的基础上也在进一步融合环境分析和行为分析策略，实现动态访问控制。

为方便理解，我们将接口保护和数据合规保护统称为 API 资产（Asset）保护，同时，将身份认证、授权管理、账号访问控制、访问审计、资产保护称为 API 访问控制的“5A 安全原则”。实践中，API 访问控制应践行 5A 安全原则，5A 策略应随 API 的交付部署到相应的访问控制系统中，对于违反访问规则的行为，直接应用阻断、限流、限速、加密、脱敏等控制措施。

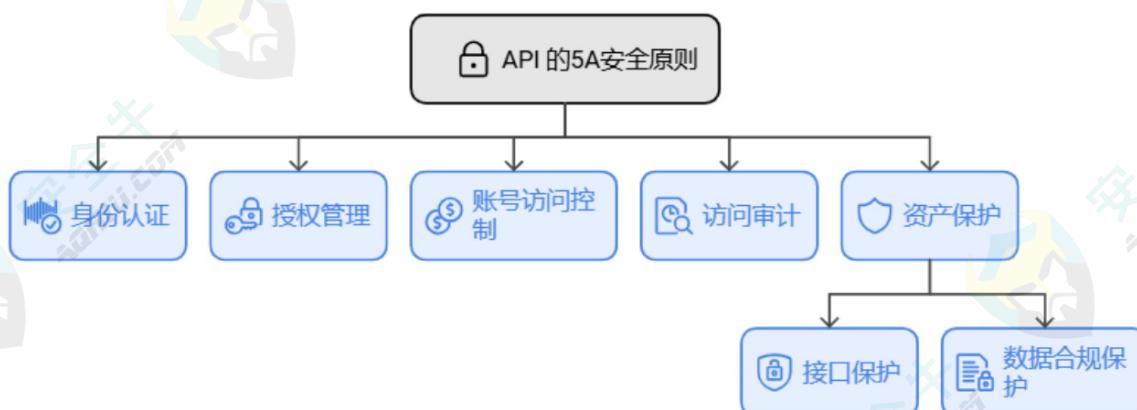


图 7 API 的 5A 安全原则

常见的实现 API 访问控制能力的产品有：API 访问代理、API 访问控制网关。

2.2.2 资产识别

资产识别是 API 风险监测的基础。API 资产包括 API 接口及其承载的应用数据，为能更好地进行 API 风险分析和定位，资产识别时还需要识别承载 API 接口的应用。

API 资产发现可以采用多种技术手段实现自动化的 API 识别，常用的发现技术有：流量分析、自动化扫描。它能通过一系列预定义的发现规则和标识规则自动化识别大部分的 API 资产，并对 API 资产类型进行区分，进而对 API 资产进行聚合、拆分等聚类管理，发现业务中的正常的、新增的、潜在的、失活的、遗留 API 和历史 API。有效地帮助运营者提高资产管理效率，快速掌握 API 资产的状态变化。

但 API 类型复杂，企业也常常有自定义的 API 接口。基于规则检测的资产发现技术，无论是流量分析还是自动化扫描技术在资产检测和梳理方面都存在一定的局限性，导致 API 识别不全、过度识别、分类标识错误等等，这会给后续的风险处置造成更严重的错误判断。因此，在资产识别过程中，经常要结合人工判断进一步提高资产发现的完整性和准确性。

在 APPI 全量识别基础上，企业通常需要进一步区分出需要重点管理的那些 API 资产，并按使用范围标识其属于私有型 API、公有型 API、混合型 API。数据资产方面，由于不同业务中数据的含义不同，数据标识时需要遵从行业数据分类分级的标准和规范。同样，对应用分类标识时也存在同样的需求。这些管理要求对当前自动化标识技术是一个较大的挑战，不能完全依赖自动化识别梳理的功能。这些都需要管理员在自动化识别的基础上进一步校正。

2.2.3 风险检测和验证

API 风险检测和验证技术是 API 风险识别的重要手段。API 风险类型多样，其中：API 脆弱性风险、网络行为风险、访问异常风险及数据风险 4 个主要的 API 风险类型。

(1) API 脆弱性风险

API 漏洞和脆弱性是应用系统的重要安全隐患，包括：常见的 WEB 漏洞风险（如 SQL 注入、跨站脚本、文件上传漏洞等），OWASP TOP10 的验证权限类漏洞（如验证绕过，授权失效等）等等。这些隐患有的是来自开发过程中不规范的开发习惯，有的是部署过程中遗留的过期或影子 API。这些接口都极易发生 API 漏洞利用风险。

运营阶段的 API 漏洞检测技术是一种被动扫描技术，它通过监听会话交互过程，分析会话上下文的行为特征、数据流和响应，寻找潜在的安全漏洞和问题。这种漏洞扫描技术不同于应用漏洞和主机漏洞扫描，它将产生大量误报，检测结果不适用于直接防护，需要通过漏洞验证确保漏洞的真实性和可利用性。

(2) 网络攻击行为

WEB 应用型 API 面临着 WEB 网站所有的网络攻击行为。包括：注入攻击、XSS 攻击、中间人攻击、Bot 攻击、DDoS 攻击等。需要结合基于规则和签名的检测，基于异常行为分析、行为特征分析、行为学习模型等攻击检测技术进行识别。

(3) 异常访问行为

异常访问行为风险是在信息系统中出现的不符合正常操作模式的行为，这些行为可能对数据安全和系统完整性构成威胁。包括：非工作时间的访问、频繁或超出正常需求的访问以及大量敏感信息数据的下载等。即使在建立了身份认证、访问授权和敏感数据保护机制的情况下，拥有权限的用户仍可能进行非法的数据查询、修

改或下载操作，这些行为往往未超出账号权限，容易被管理者忽视。

UEBA（用户和实体行为）分析、语境分析是异常访问风险检测的主要手段。

异常访问风险防护多会回归到访问控制策略上，根据 API 接口的敏感等级采取细粒度、多层次的访问控制策略，确保数据安全和系统的完整性。

(4) API 数据风险

API 接口涉及大量的用户数据和敏感信息，API 数据风险包括：数据泄露和滥用、过度数据暴露、低频数据泄露、不安全的数据传输等。

数据分类分级和涉敏数据标识是 API 数据风险检测的主要依据，是一种数据合规性检测。相关技术可参考安全牛《数据分类分级自动化建设指南》报告。

2.2.4 风险分析和可视化

风险分析和可视化是执行 API 风险评估、细粒度风险管理的重要依据。风险可视化技术利用数据和图形化展示的方式，直观地呈现 API 面临的各种风险，如 API 的存活状态，漏洞分布、攻击态势、数据要素流转等等，实现风险持续监测的目的。

风险分析和可视化技术包括，包括：特征匹配、行为模型、关联分析、智能图谱、神经网络、机器学习、大数据分析等技术手段。

- **特征匹配：**通过预定义的规则和模式识别异常行为；
- **行为模型：**建立正常行为模型，检测偏离正常行为的异常活动；
- **关联分析：**分析多个数据源和日志，发现潜在的威胁和异常；
- **机器学习：**通过训练模型，自动检测和响应未知威胁；
- **大数据分析：**处理和分析大规模数据集，提取有价值的安全洞察；
- **智能图谱：**利用图数据库和图算法，揭示复杂的关系和依赖；
- **神经网络：**使用深度学习技术，自动识别和分类复杂的威胁模式。

2.2.5 风险防护

API 通过结构和协议向下承接了业务访问，向上承载了数据的流转。

为保障业务访问和数据安全，API 风险防护应遵循多维度、细粒度和纵深防御原则。其防护能力包括：数据防护、接口保护、访问控制、网络攻击防护等等。由于防护能力的多样化，防护执行中往往还需要具备第三方联动防护的能力。

- **数据防护：**对敏感数据进行加密和脱敏处理，确保采集、传输过程中数据要素流转安全；
- **接口保护：**对接口执行限速、限流、禁止调用等操作，防止接口被恶意调用和滥用；
- **访问控制：**对 API 接口实施细粒度的身份认证、授权管理和会话管理，确保只有授权用户和应用可以访问 API，避免违规和非法访问；
- **网络攻击防护：**通过流量防护技术、网关类防护技术对恶意攻击实施阻断，防止攻击在系统内部扩散。

2.2.6 风险响应

API 的风险响应是在 API 风险事件发生后，为遏制威胁态势进一步蔓延，减少风险影响的范围和损失而采取的一系列的安全措施。包括：事件审计、风险评估，通过风险回归流程和机制采取进一步的漏洞加固、漏洞回归、访问控制和风险防御策略，完善应急响应预案等等。这可以帮助组织建立闭环的 API 风险响应体系，从事前预防、事中应对到事后改进，持续提升 API 的安全性和韧性，有效应对不断变化的风险环境，最大限度地保护组织的业务和数据安全。

第三章 应用现状及场景化分析

3.1 API 安全需求及应用现状调研

为深入了解当前国内行业用户的需求及应用现状，报告研究中基于谷安研究院的甲方客户资源开展了应用现状调研。本次调研覆盖了金融、制造、政府、运营商、互联网、能源、医疗共 7 个行业。

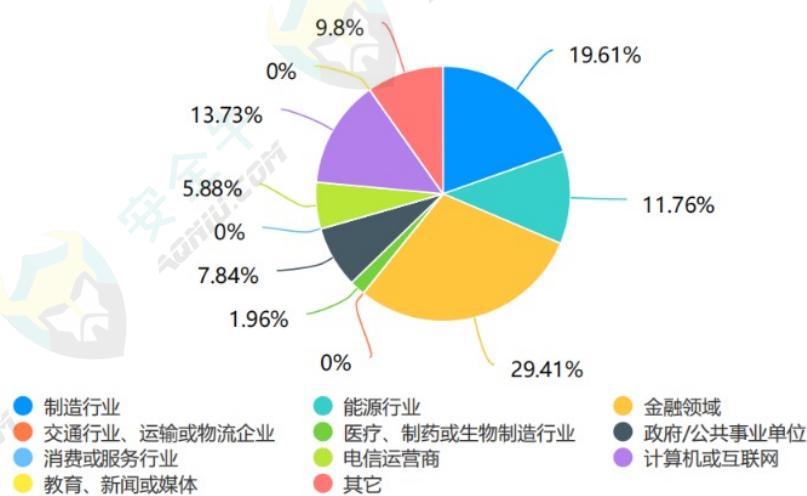


图 8 受访者行业分布情况

从受访用户的行业分布来看，金融领域用户的比例最高，占到 29.4%；其次是制造行业和计算机或互联网行业，占比分别是 19.6% 和 13.7%；能源和政府 / 公共事业单位的受访者占比分别为 11.8% 和 7.8%；运营商用户占比 5.9%，医疗用户占比约 2%。受访人群中，58.8% 来自安全规划 / 管理岗位，13.7% 是系统保障 / 运营 / 运维岗位，开发管理人员 / 工程师的比例较低，仅为 9.8%，其他岗位占比 3.9%。其中，来自千人以上规模的受访者占到了 66.6%。

这也反映了，目前阶段对软件供应链安全关注较高的企业主要集中在金融、制造业、互联网、能源、政府行业，并且较大规模的企业在市场中占据主导地位。



● 应用现状及场景化分析

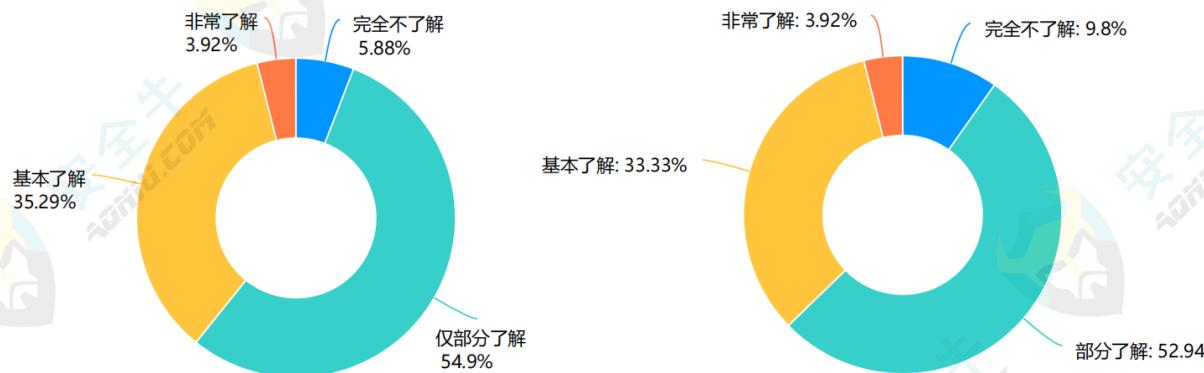
3.1.1 API 安全风险现状

API 资产是评估 API 风险的重要起点。关于企业 API 安全的现状，报告从资产、风险、攻击影响方面进行了调研。

(1) 运营者对企业 API 资产及其风险的了解程度

调研数据显示：表示“基本了解”的受访者占 35.3%，表示“仅部分了解”的受访者占 54.9%，而“完全不了解”和“非常了解”的比例都较低，分别为 5.9% 和 3.9%。同时，“基本了解”企业 API 风险的受访者占 33.3%，“部分了解”的比例为 52.9%，“完全不了解”和“非常了解”的比例分别为 9.8%，3.9%。

这表明，企业对 API 资产的了解程度还较低，尽管有 1/3 受访者表示他们对 API 风险有一定认识，但显然企业在 API 资产管理方面存在明显缺口，需要采取进一步安全知识的教育和培训，提升企业对 API 资产的了解程度，增强 API 风险评估。

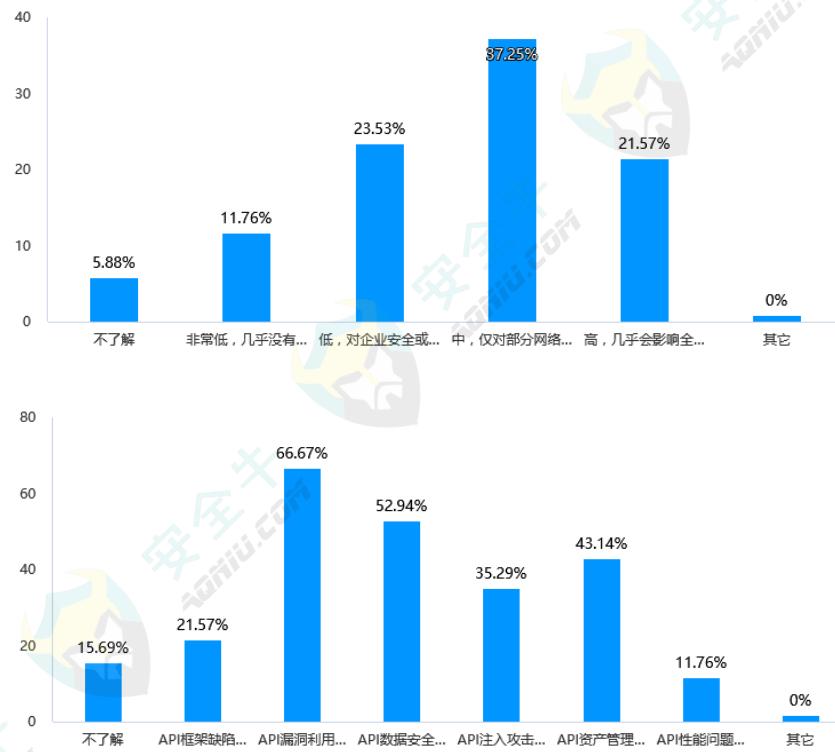


(2) API 风险对企业的影响

影响程度方面，调查数据显示：90% 以上的受访者认为 API 风险对企业有影响，但其中，认为风险影响为低和非常低的占 35% 左右，认为影响中等的占 37.3%，认为影响较高的用户占 21.6%。

风险类型方面，认为 API 漏洞利用对企业影响最大的用户占比最高，约 66.0%，数据安全风险紧随其后，占比 50.9%，API 资产管理缺失、API 注入攻击影响分别占比 41.5% 和 34.0%，API 框架缺陷和 API 性能问题的影响相对较小，占比分别为 22.6%、13.2%。

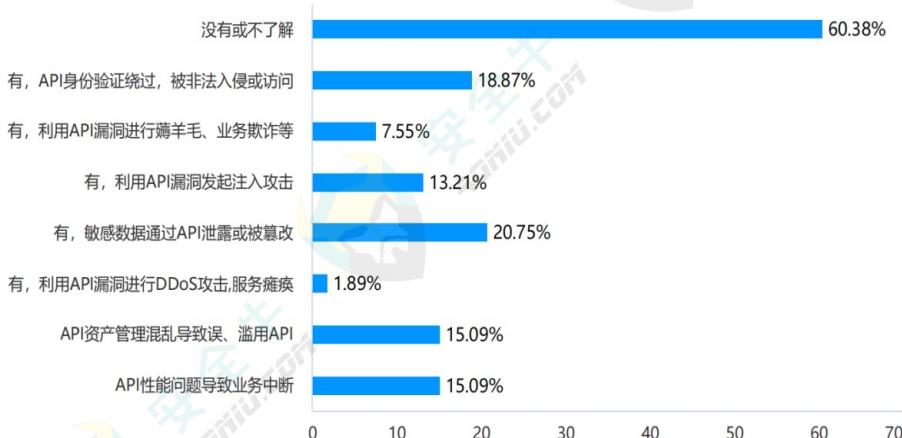
整体来看，在所有 API 风险类型中，API 引起的漏洞利用、数据安全问题对企业影响最为敏感，但大多数用户认为 API 风险对企业的影响程度处于中低水平，影响相对有限。



(3) 过去 3 年企业遭受的 API 攻击的情况

调研显示，40% 左右的调研者表示企业遭受过 API 攻击。攻击类型方面，敏感数据泄露和身份验证绕过是风险比例最高的两种问题，分别占 20.8% 和 18.9%；其次，API 资产管理混乱和 API 性能导致业务中断问题，各占 15.7%。

这组数据表示，企业在运营中会同时遭受多种类型的 API 攻击事件。其中，敏感数据、身份验证是最容易遭受攻击的两个薄弱环节；此外，API 资产管理缺失问题也正在使企业面临一些切实的安全风险。

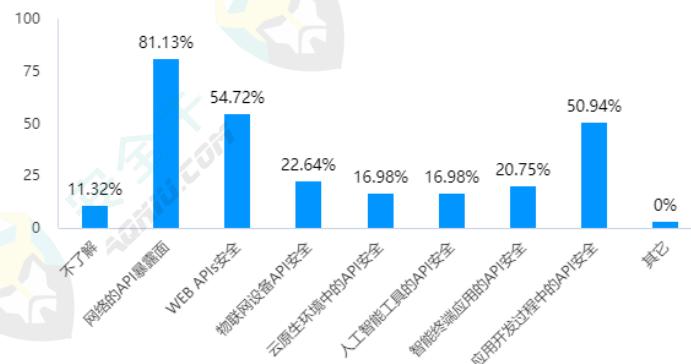


● 应用现状及场景化分析

(4) 企业最关注的 API 安全的应用场景

调研中，88% 左右的受访者表示对 API 安全有不同方面的关注。其中，API 暴露面的关注度最高，占比高达 81.1%；其次是 WEB 和开发过程中的 API 安全，关注度分别为 54.7% 和 50.9%；物联网、智能终端、云原生和人工智能领域的关注度相对较低，分别为 22.6%、20.8%、17.0%、17.0%。

这说明，用户对 API 的关注主要集中在应用、WEB 和安全开发场景中，新兴领域的关注度相对较低。但随着技术的发展，这些领域的安全问题可能会愈加突显。建议企业应提前布局，增加相关的安全策略和措施。



3.1.2 API 安全建设现状

(1) 企业实施 API 安全防护的目标

调研显示，71.7% 的受访者表示企业有实施 API 安全防护的计划，驱动因素来源于多个方面。其中，26.4% 受访者表示诉求源于法规和监管要求；24.5% 受访者表示是为了进一步提升网络安全，减少风险暴露面，防范潜在的网络攻击；此外，18.9% 企业表示是为了保障业务的连续性和可用性。但调研也显示，有少部分用户希望能通过 API 安全提升自己产品和品牌的影响力。

这表明企业实施 API 安全建设的目的不仅仅是为应对安全法规和行业监管，更多的驱动力是来自业务自身的安全需求。API 安全扭转了企业以往政策驱动的被动局面。



图 9 驱动因素调研

(2) 企业实施 API 安全能力建设会优先选择哪种类型的解决方案

API 安全方案的调查结果显示，选择“与传统防护能力融合型”和“在现有系统上升级”解决方案以 22.6% 和 20.8% 的比例占据首位；选择“独立部署的专业的 API 解决方案”的用户占比为仅为 17.0%。

这一调研反映，由于网络安全建设的深入，在 API 安全防护中，受访者更重视与已有防护能力结合。

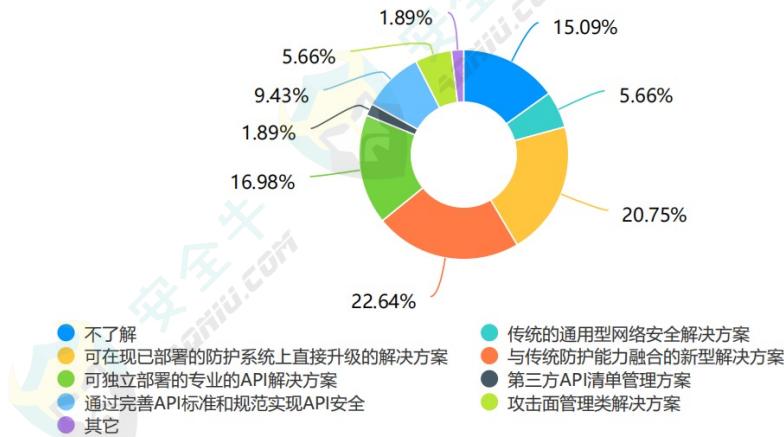


图 10 方案类型调研

(3) 目现阶段 API 安全工具的采用情况

调研显示，70% 左右的受访者表示企业采用了不同类型的 API 防护工具。

其中，WEB 漏扫或传统 WEB 防火墙的使用比例最高，达 41.5%；其次是 API 防护网关，比例为 37.7%；WAAP 类产品占比 30.2%；API 检测 / 评估工具占比为 24.5%；API 风险监测类产品的采用率在 20% 左右。

这一数据表明，企业在 API 安全建设中，检测、监测和防护类产品均有涉及，并且半数以上企业会采用两种以上类型的工具。

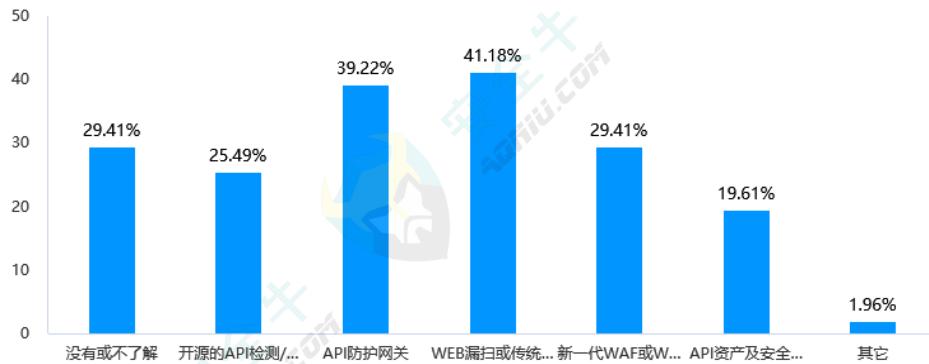


图 11 工具采用情况调研

● 应用现状及场景化分析

(4) 实践中，企业认为相对有效的 API 安全工具类型

85% 左右的受访者在调查中对工具有效性表达了明确的态度。

其中，API 网关是最受欢迎的工具，获得了 64.7% 的支持比例；API 资产识别及安全防护平台紧随其后，占比是 54.9%；其次是，API 审计、WAF，支持率分别为 35.3%、31.4%。相比之下，WAAP 和 AST 测试工具的选择比例相对较低，分别为 13.73% 和 9.8%。

这一数据显示，API 网关、API 安全监测平台被认为是最有效果的两个产品类型，但应用防护、审计、测试验证也是 API 安全体系中必不可少的能力。

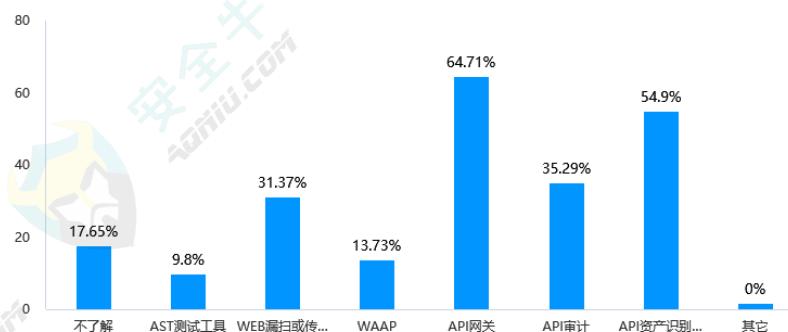


图 12 工具有效性调查

(5) 企业应对 API 身份验证失效问题的措施

调查中，75% 左右的受访者表示了解企业在应对 API 身份验证失效问题方面的相关措施。

其中，多因素认证比例最高，达到 54.7%；其次，令牌认证、OAuth 协议、证书也占据了较大的比例，分别为 39.6%、37.7%、32.1%。相应地，API 共享密钥和客户端证书的采用比例较低，分别为 18.9%。

这表明，在应对 API 接口身份验证失效问题上，企业更愿意采用安全性更好的认证方式，共享密码实施简单，但可能由于安全性和密钥分发问题，支持率较低。

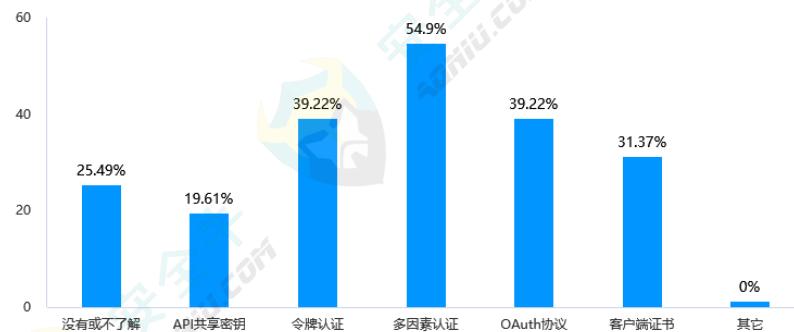


图 13 API 身份验证方式调查

(6) 企业当前缓解 API 数据泄露和非法访问问题措施

调查中，80% 左右的受访者表示了解企业当前在 API 数据访问、泄露方面的应对措施。

其中，采用数据加密 / 脱敏、授权和访问控制策略、网络防护措施的占比最多，分别为 58.5%、54.7%、50.9%，而部署 API 自动化审计和溯源工具，对 API 访问行为进行监控的比例较低，仅 28.3%。

这一调查显示，数据安全防护大于预防，加密、脱敏和访问控制仍是企业当前 API 数据安全防护的主要手段。

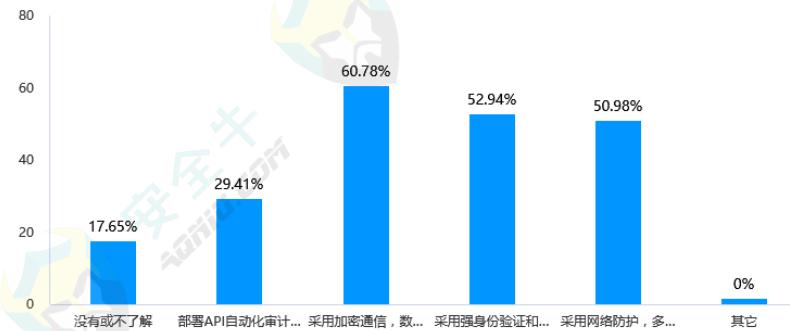


图 14 API 数据安全防护调查

(7) 从 API 生存周期来看，哪一阶段的 API 治理能更有效地缓解 API 风险

调查显示，认为在应用设计、开发阶段采取相关措施更有效的比例最高，达到 41.5%；其次是日常运行中的风险监管和防护，占比 18.9%。相比之下，进行 API 安全相关培训、上线前的验收测试、API 的配置管理在缓解 API 安全有效性方面的支持率较低，分别是 15.1%、13.2% 和 3.8%。

这也说明，尽管企业更重视 API 使用周期的风险防护，但在风险治理方面。更希望从开发、设计阶段就加强风险管理，减少 API 自身的脆弱性。

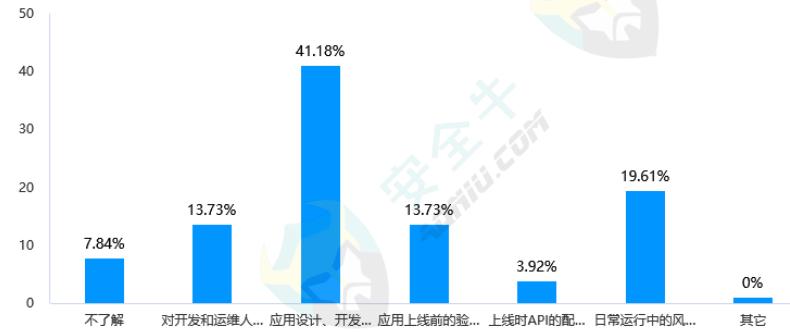


图 15 API 安全周期

(8) 企业 API 安全能力建设中可接受的支出预算

调研中，超过 50% 的受访者表示不了解或没有相关建设计划，并且 30.2% 的受访者明确表示没有计

● 应用现状及场景化分析

划。而在有计划的企业中，只能提供 30 万以下建设支出的比例约 24.0%，能提供 30 万以上支出的比例为 20.1%。

这组数据表明，大多数企业的 API 安全建设还未提上日程，观望者居多，预算整体分布情况也偏保守。

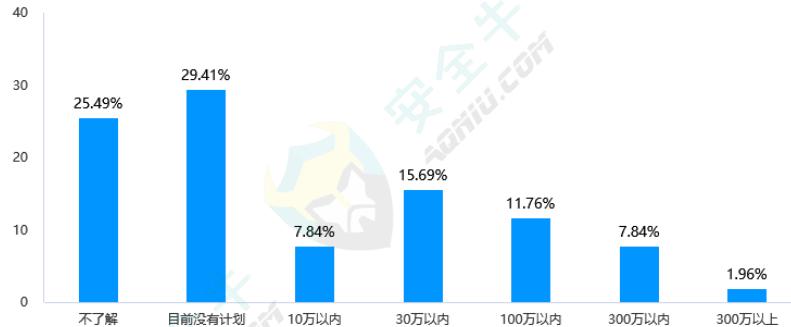


图 16 建设预算

3.1.3 API 安全建设挑战

API 安全是一个新兴领域，用户在方案选型和方案落地过程中难免会面临各种挑战。报告从方案、供应商和建设三个方面对建设挑战进行了观察。

(1) 企业在选择 API 方案和产品时的关注点

调查显示：企业在选择 API 方案和产品时，对功能完善度和易用性关注的占比最高，达到 79.3%；其次是系统化、场景化应用能力，占比 81.1%；厂商服务能力占比 66.1%。相比之下，创新性和品牌影响力占比明显低一些，分别为 30.2%、20.8%。

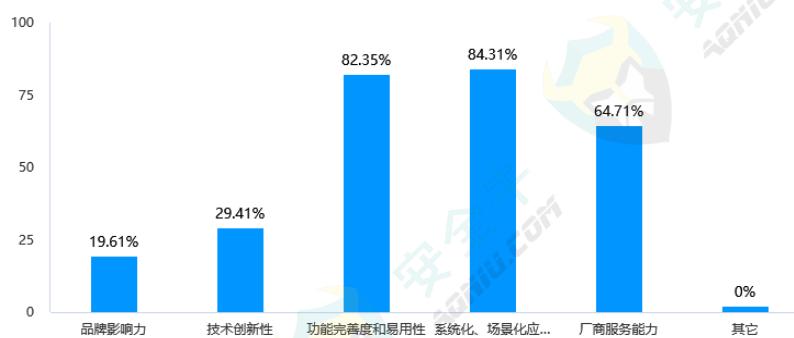


图 17 API 方案和产品

这组调查数据显示，在 API 安全方案选择时，用户会更多追求产品的成熟度和适用性，而不是创新性和品牌影响。

(2) 企业在选择 API 安全方案和提供商时的挑战

调研中，有 80% 左右的受访者表达了相应的观点。

其中，认为厂商方案不能与企业已有的安全建设有效融合，易导致重复建设的比例最高，达到 56.9%；其次是场景匹配度不高，体系化能力不足，占比分别是 43.1%、41.2%；此外，还有近 1/3 的受访者表示对厂商缺乏了解，27.5% 的受访者表示成本在采购决策方面也有一定影响。

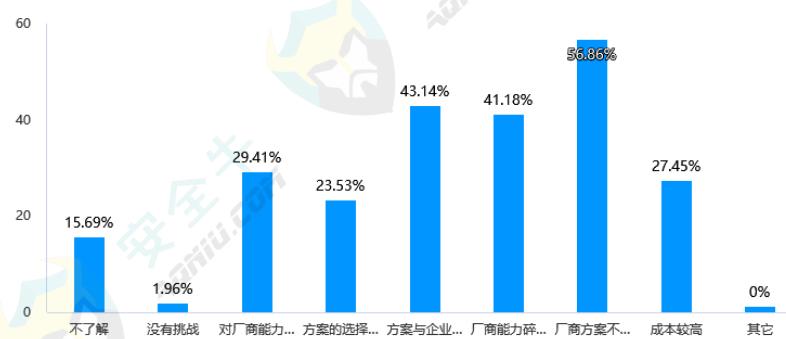


图 18 供应商选择过程中的挑战

这表明，企业在寻找适合的方案和厂商过程中存在多方面的困难，而系统融合性、场景匹配性、风险一体化管理方面的问题最为显著。

(3) API 在安全建设阶段的困难

调查显示，企业在 API 建设过程中还存在多方面的困难，具体体现在技术、管理体系建设、运营、场景覆盖 4 个方面。

技术方面，半数的受访者认为 API 资产难以梳理，风险难以评估；22.6% 的人认为现有工具难以覆盖 API 安全的场景化需求；24.5% 的人提到难以与已有的安全系统集成和融合，导致资源浪费和效率的低下。

管理体系建设方面，37.7% 的受访者表示缺乏有效的 API 安全管理制度和流程，28.3% 的受访者提到开发团队的安全意识和技能欠缺，团队培训和意识提升方面需要加强。

运营方面，1/3 左右的受访者认为 API 策略复杂，运营难度较大，并且缺少专业的 API 安全人才；24.5% 的受访者提到 API 业务变动频繁，安全策略难以同步；还有 17.0% 的受访者担心 API 防护引入后对业务性能的影响。

● 应用现状及场景化分析

此外，22.6% 的受访者认为安全投入与收益难以平衡。

整体来看，在技术和运维方面的问题较为明显，特别是资产梳理和风险评估。这可能导致安全策略的执行力不足，进而影响整体安全水平。

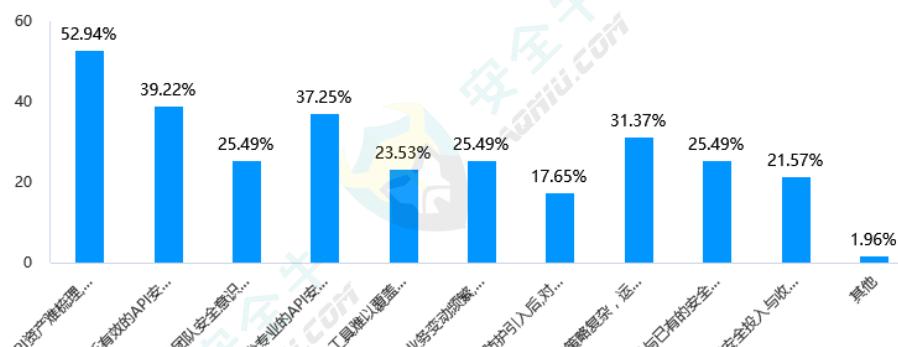


图 19 建设阶段挑战

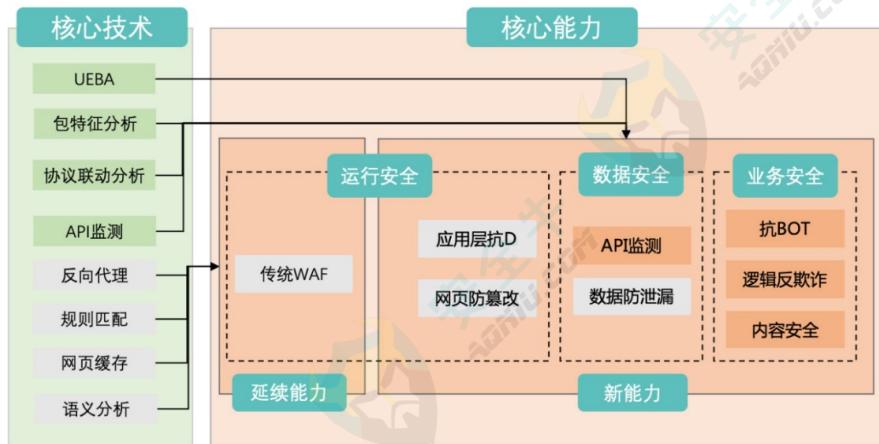
3.2 API 安全的典型应用场景分析

API 安全应用非常广泛，可以覆盖网络安全、应用安全、业务安全、数据安全多个场景。报告选取了典 WEB 安全防护、微服务治理、业务风控、数据要素流通管控、网络安全 5 个典型场景进行分析。

3.2.1 API 安全与 WEB 安全防护

随着 WEB 服务的兴起，互联网企业都开始采用 WEB 页面向用户传递企业的服务价值，WEB 页面对外开放的接口越来越多。WEB APIs 承接了 WEB 页面所有的数据访问。随着 WEB 数据价值的提升，针对 WEB 的攻击也逐渐从 WEB 页面攻击转向了 WEB APIs 的定向攻击，如通过 WEB 访问向 WEB APIs 发起各种注入攻击，利用 API 接口脆弱性实施越权访问，窃取敏感信息等等。这将给 WEB 系统及 WEB 服务造成严重的影响。因此，基于 WEB 的 APIs 防护必须成为当前 WEB 安全的重点内容。

传统的 WEB 安全防护产品通过无法识别 WEB APIs 漏洞利用和数据泄露风险。为保障 WEB 安全的有效性，需要在传统 WEB 攻击检测和防护的基础上，增加 API 的风险检测和防护能力，并构建一个多层次的 WEB 安全防护体系，涵盖从 WEB 访问到 WEB 页面、WEB APIs、WEB 数据的新 WEB 安全防护能力。



图片来源：安全牛《新一代 WAF 技术应用指南》

图 20 API 安全与 WEB 防护

WEB 安全防护场景中的 API 安全能力，详细内容可请参考安全牛《新一代 WAF 技术应用指南》报告。

3.2.2 API 安全与微服务治理

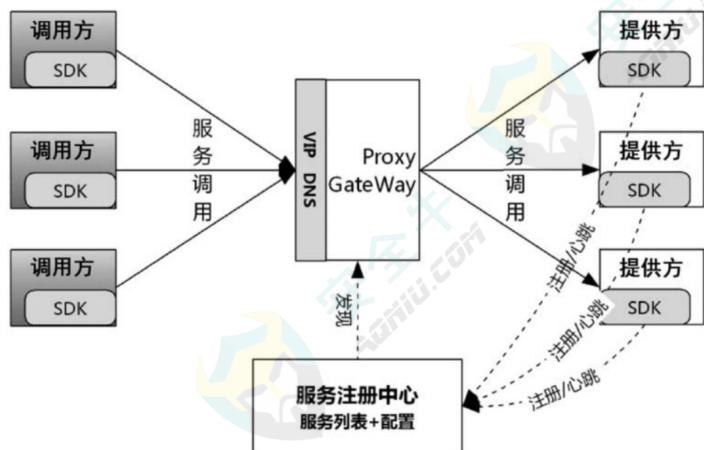
随着云服务的发展，微服务架构成为当前的主流开发模式。微服务在云环境中以服务实例方式独立部署和维护，业务和服务、服务和服务之间通过网络调用的方式进行通信，调用双方遵循“服务接口契约”，即我们常说的服务 API。

微服务开发者面向不同的业务客户提供共享服务，专注于特定的功能，并不考虑业务逻辑的特殊需求，服务 API 和数据的安全策略都需要根据业务和环境需求进行配置。

从调用者角度，任何一个微服务的工作模式、安全性都会影响整体的业务运转。在云开发环境下，对微服务进行服务注册发现、实施安全访问策略、集中进行风险监测和管控，可以简化业务开发，提高业务开发的效率和可靠性。

API 网关是微服务治理的代表性产品。作为微服务架构中服务接入的统一入口点，API 网关可以承担攻击防护、接入访问、数据访问等安全管理职能。通过集中管理的安全策略，能对服务 API 版本进行有效性管理，应对针对 API 接口的攻击，防止未经授权的访问和恶意请求，监测涉敏涉密数据流转，实施数据泄露防护等等，从而提高微服务系统整体的安全性。

● 应用现状及场景化分析



图片来源：《微服务治理：体系、架构及实践》

图 21 API 安全与微服务治理

3.2.3 API 安全与数据要素流通管控

2020 年 4 月，国务院发布《关于构建更加完善的要素市场化配置体制机制的意见》首次提出了数据要素，并提出培育数据要素市场。为推动数据要素市场的建设和发展，国家在 2021 年发布《“十四五”数字经济发展规划》提出数据要素市场的发展目标，到 2025 年初步建立数据要素市场体系。2022 年 12 月，国务院进一步发布《关于构建数据基础制度更好发挥数据要素作用的意见》也称“数据二十条”，建立了数据要素的整体框架，涵盖：数据产权制度、数据要素流通和交易制度、数据要素收益分配制度和数据要素治理制度四个构建数据基础制度的核心制度。可见，实施数据要素治理加强数据要素流通管控是加快数据要素市场化流通，推动我国数字经济高质量发展的重要前提。

技术上，数字身份、隐私计算、区块链等在构建可信数据流通架构中都发挥了重要作用，提高了数据流通交易的安全性、稳定性和便捷性。但 API 作为数据传输和共享的重要通道，API 的暴露及其面临的风险直接影响到数据要素的流通和管理。传统的安全能力不能有效覆盖 API 接口及其数据要素细粒度管控的需求。为应对该挑战，API 安全管控也被广泛应用于数据要素流通中。

API 安全管控可以从接口安全、数据安全、审计三个方面为数据要素流转构建 API 接口的防护面。一方面通过身份验证、数据加密、访问控制、实时监控等手段，确保 API 接口的安全性和数据的完整性；另一方面，在 API 安全管控过程中可以直接应用数据脱敏和隐私保护等数据安全策略，有效防止数据流转过程中敏感数据的泄露；另外，API 安全管控可以对 API 出入数据实施数据合规审计，有效预防数据流转风险，提高事件溯源和分析能力。

API 安全在数据要素治理中不仅可以保障数据要素流通，为数据要素市场健康发展提供支撑，也有助于进一步实现可信、透明和可计量的数据共享和交易。



图 22 数据要素流转管控

3.2.4 API 安全与业务风控

随着网络经济的发展，业务风险、支付交易安全成为现代电子商务和金融交易的关键问题。业务风控能有效预防虚假账号、盗用资金、营销作弊、违约欺诈和身份伪造等风险，避免资金损失、用户流失和商誉损害。随着数据安全法、个人信息保护法及数据监管政策的出台，数据安全合规对业务风控也提出了更高的要求。

API 是业务交易过程中个人信息、敏感数据流转的重要关口。API 接口安全不仅关系到业务安全运行，还直接影响到客户隐私安全和企业数据安全合规问题。在业务风控中实施 API 安全管理，可以更细粒度地实现业务风险暴露面管理，在事前识别逻辑调用行为预防业务风险，在事中对涉敏数据流转实施管控和脱敏处理避免数据泄露，在事后对数据风险事件进行溯源分析降低企业损失。

业务风控应用场景非常广泛，不同场景的风控模型不同。如在金融领域，风控更多考虑用户的信贷风险和敏感数据；而在电商平台，则可能更关注交易欺诈、恶意流量和账号安全。这要求 API 安全能融入企业风控管理体系之中，并为不同场景的业务风控需求提供安全支撑。

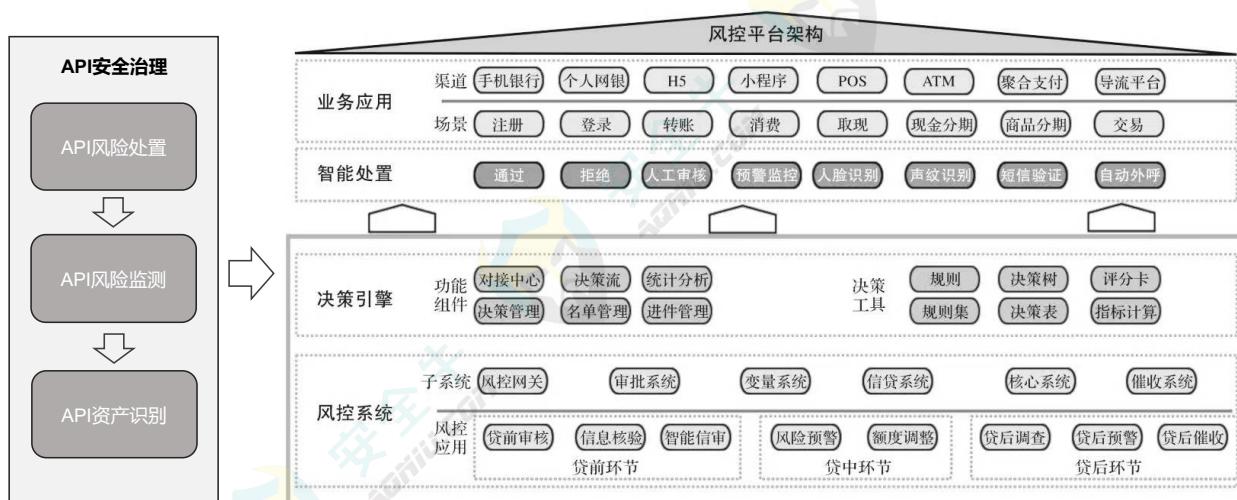


图 23 API 安全与业务风控

● 应用现状及场景化分析

3.2.5 API 安全与网络安全

随着数字化转型的深入，企业不断开放南北向接口和东西向接口以实现更丰富的业务连接能力。这些面向互联网的南北向接口给企业制造了巨大的暴露面，成为攻击队选手的首要突破口；同时，企业内部业务之间 API 接口的脆弱性，也给攻击者在突破边界后向内部系统横向渗透提供了机会。

API 安全通过流量分析的方式识别 API 资产和风险，这可以实现企业南北向、东西向接口的统一管理。结合 API 安全细粒度的访问控制、风险检测（攻击、脆弱性、行为）、事件溯源、数据流转分析能力可以为网络安全方面提供更全面、更细致的攻击面管理。在访问流量串行的模式下，也可以进一步发挥 API 安全访问控制的优势，助力企业进一步实现零信任网络。

API 的安全能力在网络安全方面能进一步提升企业实施攻击管理、零信任网络访问和攻防演练的有效性。即适用于传统的企业环境，也适用于云原生环境的安全管理。

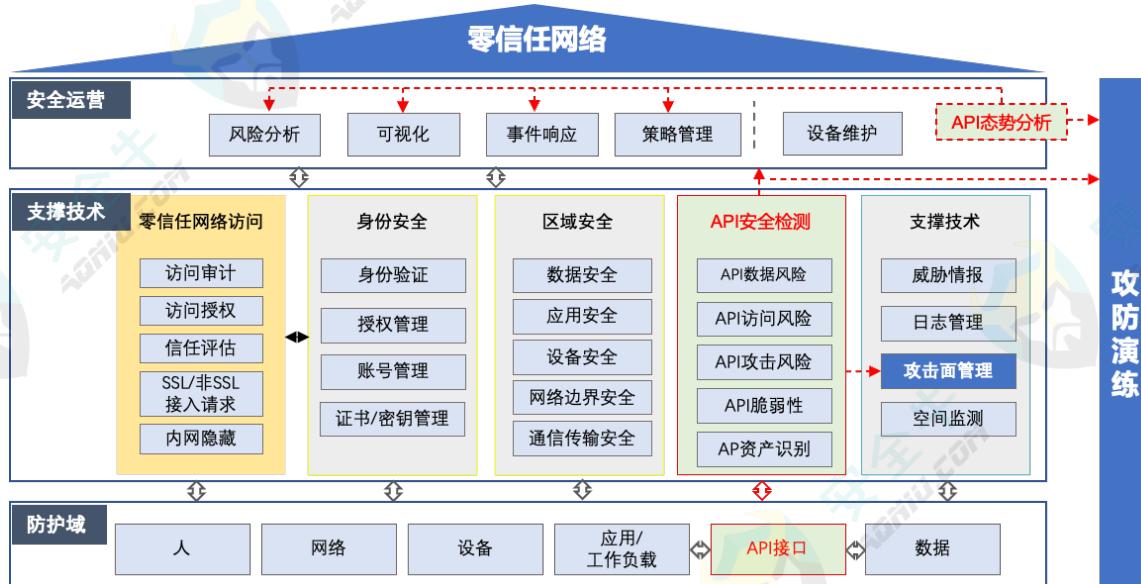


图 24 API 安全与网络安全

第四章 API 安全建设指南

4.1 建设挑战

由于 API 应用的广泛性、类型多样化及防护技术的复杂性，API 安全防护难度普遍被认为是较高。根据走访调研，安全建设过程中，企业在技术、流程、安全运营方面都存在诸多困难，其中的主要挑战包括资产识别、风险防护、涉敏数据标识和安全运营 4 个方面。



图 25 API 安全建设挑战

(一) API 资产识别和梳理的准确性挑战

首先，随着企业数字化转型的推进，API 数量在呈爆炸式增长，并广泛分布于应用、系统、WEB 页面等数字资产。根据服务范围，API 又分为公有型 API、私有型 API 及混合型 API，加上云上云下混合部署方式，导致多数企业对其环境中存在的 API 数量及其具体用途缺乏清晰认识，难以梳理出全面的 API 资产清单。

另外，为了便于企业对 API 资产有重点的管理，API 接口梳理过程中需要进一步结合应用分类、敏感数据管理知识，并做好资产之间的关联关系。尽管目前自动化的资产识别和关联分析能力能提高资产梳理的效率，但为保证资产识别的准确性，过程中还需要人工调整甚至手工配置难以识别的一些 API 接口。

(二) API 防护的挑战

首先，API 安全需要多样化的风险检测手段。由于 API 部署的复杂性，API 面临的风险也更复杂。涉及接口自身的漏洞利用、内部员工滥用权限、外部攻击和异常访问以及敏感数据流转风险。满足这些检测需求需要融合漏洞挖掘、访问控制、攻击检测及数据安全的能力，对单一厂商的能力要求较高。

其次，API 风险无论是漏洞还是攻击都非常依赖流量采集和行为分析。流量采集的全面性、流量中的噪声会严重影响风险检测水平；特别地，API 在负载状态下，尤其是在大流量环境中，流量解析、API 的并发处理都需要更高效的数据处理和分析算法；检测策略方面，行为规则的细度、行为模型的训练精度都会有一定的漏报和误报。

API 风险检测的准确性导致风险防护不能完全自动化，即使相对确凿的风险，很多时候也会由于防护手段缺失无法实施有效防护。比如，旁路部署的流量探针在阻断时往往有一定的失误率，并且不能对 API 接口进行细粒度的专业处置；还有 API 漏洞问题，通常没有补丁或热补丁策略，需要进一步左移到开发寻求解决方案。

(三) API 涉敏数据精准识别难

首先，涉敏数据包括与个人相关的敏感数据和行业相关的密级数据。涉敏数据识别需要遵循个人信息保护法、数据安全法及行业数据分类分级标准和规范，结合业务需求因地制宜的配置涉敏标识规则。涉敏数据标识错误会导致数据识别错误，给数据处理造成困扰甚至方向性错误处置。

其次，API 上传递的数据比起 SQL 这种格式固定的语言更加多变，语义也因不同的实现者而变得多样且丰富。API 敏感数据识别时，还需要结合语义分析正确地理解数据的行为，才能搞清要如何防护。

(四) API 安全的专业运营人才奇缺

API 风险检测和防护技术方面的短板，导致 API 安全对安全运营有较高的依赖。但 API 安全运营需要对应用和业务、API 协议、数据安全知识都相对全面的安全人才。这导致尽管许多企业意识到 API 安全在安全运营中的重要性，但仍然由于缺乏专业的安全运营人才，导致 API 安全防护工作不能有效开展。

4.2 基本建设原则

API 是随着网络安全建设不断完善和攻防对抗技术的进一步增强，逐步暴露出来的一个新安全建设盲区。绝大多数企业对 API 安全建设都缺少经验。结合安全牛的 API 安全治理框架，报告提出了 API 安全建设的 4 项基本原则。



图 26 API 安全建设 4 项基本原则

(一) API 安全建设要有章可循 从源头抓起

API 安全操作规范和安全指南，可以提高管理者的 API 安全意识和防护知识，为 API 开发、部署提供基本的安全指导，确保 API 安全建设有章可循，是落实并推进 API 安全建设重要前提。

将 API 安全操作规范和安全指南纳入 API 安全治理体系，特别是从开发和设计阶段就注重 API 安全性，确保遵从 API 安全开发原则，是目前国际 API 服务提供商的普遍做法，也是公认的 API 安全最佳实践。目前国际权威的 API 安全指南，包括：

《Swagger RESTful API 文档规范》即 OpenAPI 规范，描述了创建 RESTful 架构的 API 所要遵循的原则与规范，帮助开发人员和用户更好地理解和使用 API。

《OWASP 安全编码规范快速参考指南》该指南提供了更详细的编码安全实践，帮助开发人员在软件开发生命周期中集成安全性避免常见的安全漏洞。

(二) API 防护能力建设 遵循纵深防护和闭环管理的原则

首先，API 的风险是多方面的，不仅有 API 自身的脆弱性风险，还关联了应用、数据和业务的风险，这决定防护 API 风险时需要一个全面的、多层次的防护处置策略，不能仅依赖单一的安全措施。具体来说，API 的安全防护应纳入整个网络安全的纵深防护体系中，从网络访问、应用防护、接口防护、数据防护多个层面构建多层的 API 安全防护机制。

其次，API 防护能力建设要从资产识别做起，遵循“识别 - 防护 - 检测 - 处置”（IPDR）的风险闭环管理原则，保障防护能力的有效性和持续性。同时，在 IPDR 中结合零信任的理念，运用权限最小化、动态访问等技术建立可信的、自适应的可信访问机制，以更好地应对不断变化的、未知的安全威胁。

(三) API 安全要坚持左移 由被动防御变主动防御的原则

API 风险防护的滞后性决定 API 安全需要从全生命周期着手，在事前引入更多安全考量，而不是在事后寻找补救措施。因此，API 安全要坚持左移以及由被动防御变主动防御的原则，将安全措施前置。以下是实施 API 安全左移时可以参考的几个方面：

首先，在 API 漏洞管理方面，采用相应工具（如，漏洞管理平台）打通组织的流程壁垒，建立 API 漏洞监测与漏洞修复加固的机制。将 API 安全纳入应用设计和开发阶段，融入 DevOps 流程以确保在漏洞发现后能快速找到相应解决方案，从根本上提升 API 自身的免疫力。

其次，在 API 发布过程中，同步实施 API 安全策略，建立 API 安全基线。包括 API 的访问控制和身份认证、细粒度管理 API 权限配置、API 的输入验证和数据加密传输、对 API 返回的敏感数据进行脱敏处理等等。这些

策略能有效防御常见的异常访问，注入、跨站脚本类攻击，避免隐私信息泄露。

最后，做好 API 安全审计，增强事前预防和事后溯源的能力。包括：API 访问合规策略审计、数据安全合规策略审计、API 访问行为审计、API 数据流转审计及风险事件审计等。安全审计可以促进企业完善合规管理，发现潜在的安全问题，提前采取预防措施增强系统韧性，使企业安全防御由被动变主动。从行业监管角度，也建议进一步完善 API 安全合规要求，将 API 安全纳入监管体系，并落实 API 安全合规审计制度，促进企业 API 安全审计能力落地，提升整体 API 风险治理的有效性。

(四) API 安全要遵循同步建设、同步运营的原则

API 的资产类型和风险特征复杂，仅靠上线时配置的安全策略无法满足资产识别和风险检测的准确度。需要通过运维确认并校对系统自动识别出来的 API 资产的准确性。同时，还要基于业务运行态调优安全策略，改进风险算法和模型提高检测的准确性，甚至要结合风险类型修改响应处置方式。最终形成一套与业务场景吻合的、常态化的检测规则和运营机制。

因此，API 安全要遵循“同步建设 同步运营”原则，通过精细化的运营服务持续提升 API 检测的有效性和风险处置的实时性。这也要求运营人员的安全知识和业务知识都要全面。企业需要加强安全运营与业务部门合作，定期开展业务安全知识培训和防护演练，提升 API 安全持续运营能力。

4.3 方案选择建议

目前，市场上 API 安全方案的类型多样化，用户在选择 API 安全方案时，需要结合企业的安全需求和具体业务特点选择适合的方案。为方便识别厂商能力和方案特点，报告将本次调研过程中的方案分为访问控制网关类、风险监测类和数据流转管控类三种类型。其中，风险监测类方案的厂商最多，如图 27 所示。

访问控制网关类	风险监测类	数据流转管控类
<ul style="list-style-type: none"> • 美创科技 • 青笠科技（新） • 大拙信息（新） • 九州云腾 	<ul style="list-style-type: none"> • 绿盟科技 • 瑞数信息 • 奇安信 • 柳柳安全 • 安天 • 芯盾时代 • 长亭科技 • 迪普科技 • 安胜华信（新） • 喜数科技（新） 	<ul style="list-style-type: none"> • 闪捷信息 • 观安信息 • 石犀科技（新）

图 27 方案类型及代表性厂商

(一) API 访问控制网关类

API 访问控制网关类方案主要关注 API 的访问控制，提供访问控制规则、身份认证、授权管理、数据加密、涉敏数据管控、API 接口流量控制等功能，确保只有合法的用户和应用可以访问 API。

方案特点：

- (1) 安全策略侧重于接口访问合规、数据访问合规，对于违规访问行为可以实现 API 接口的细粒度管控，如阻断，限流、限速，脱敏、加密等。
- (2) 适用于对应用（API）集中访问管理场景，如零信任访问控制、应用（API）发布管理、服务治理等。
- (3) 部署方式以流量串行部署为主。
- (4) 提供该类方案的代表性厂商有：美创科技、青笠科技、大拙信息、九州云腾。其中，青笠科技、大拙信息是该领域的创新厂商。

(二) API 风险监测类

API 风险监测类方案主要关注 API 资产风险监测和风险防护，提供实时监控、攻击检测、异常检测、日志记录、风险告警、审计报告、风险防护等功能，帮助用户及时发现和应对网络安全事件。

方案特点：

- (1) 相比访问控制网关，该类产品更侧重于网络攻击、漏洞利用、行为风险和数据风险的检测，安全策略以行为规则和行为检测为主，告警有一定误报率。
- (2) 风险处置多通过联动网关类设备实现，部分厂商会将传统的 WAF 功能直接集成进来，以提高自动化风险防护能力。但相比网关类产品，该类产品对 API 接口风险的细粒度防护能力有限。
- (3) 该方案与业务安全管理的耦合度较低，应用相对广泛，可用于支撑网络安全防护，如攻防演练、攻击面管理，也可以用于支持业务风控及数据风控。
- (4) 部署方式多以旁路部署为主，通过流量镜像或部署流量探针的方式将流量牵引到监测平台；
- (5) 该类方案厂商多来自传统的网络安全能力提供商，代表性厂商有：绿盟科技、瑞数信息、奇安信、梆梆安全、安天、芯盾时代、长亭科技、迪普科技、安胜华信、喜数科技。其中，安胜华信、喜数科技是该领域的创新厂商。

(三) API 数据流转管控类

API 数据安全流转管控类方案主要关注 API 接口的数据安全流转问题，提供数据加密、脱敏、访问控制等功能，确保敏感数据在传输和存储过程中的安全性。

方案特点：

- (1) 该类方案在安全策略上与数据安全策略紧耦合，适用于数据流动管控要求较高的场景，如业务风控、数据交易、数据要素流转等。
- (2) 在监测场景下，该方案可以旁路部署，在需要对数据强管控场景下采用流量串行部署的方式。
- (3) 该类方案的提供商以传统数据安全能力厂商为主，代表性厂商包括：闪捷信息、观安信息、石犀科技。其中，石犀科技是该领域的创新厂商。

以上三种方案也分别体现了厂商对 API 安全产品的不同定位。尽管不同方案的功能侧重和场景应用各异，但调研中我们发现，几乎所有类型产品都在 API 资产识别功能中提供了数据资产识别及数据分类标识的功能。这预示着，API 安全将有可能成为数据流转合规的一项标准化的管理手段。

4.4 年度代表性供应商介绍

API 安全供应商选择方面，安全牛建议结合厂商的综合能力和技术细分能力进行评估，如图 28 所示。

- **厂商综合能力参考：**品牌影响、技术能力、产品化能力、方案能力和服务能力 5 个维度；
- **技术能力评估参考：**API 资产识别和梳理、API 脆弱性发现、API 攻击和异常行为检测、API 数据风险检测、API 风险防护处置 5 个核心能力指标。

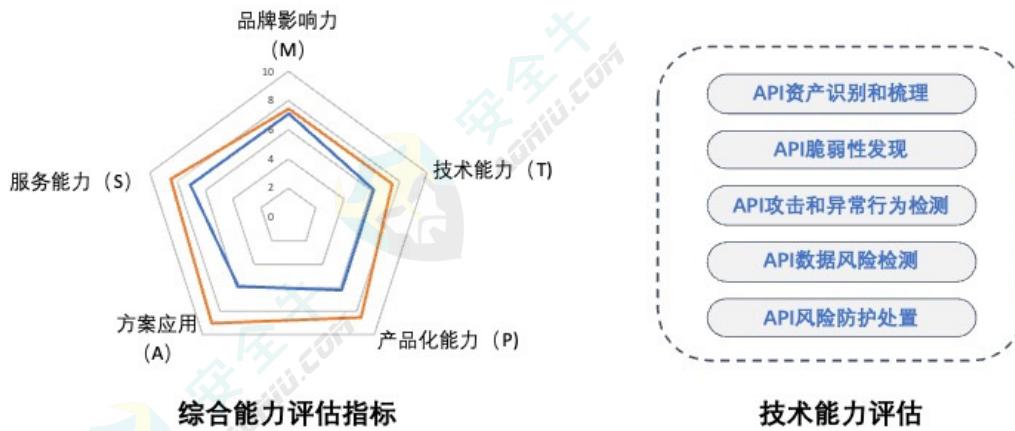


图 28 供应商选择

为了解 API 安全不同厂商的技术和产品实现情况，安全牛对该领域厂商进行了走访式调查，同时结合问卷、线上访谈、产品演示的方式对厂商能力进行了综合能力评估。具体评估方法如下：

- 评估方法为描述性评估，结合了问卷、访谈、产品演示、定性和定量评估多种方式；
- 采用了两级评估指标，其中一级指标 5 个，二级指标 20 个，涵盖评分点共 41 个；
- 评估结果以 5 维雷达图和综合评价两种方式展示。

本次调研中有 19 家厂商申报，根据问卷完整度最终有效调研厂商 17 家。

厂商侧调研显示，API 安全作为一个新兴赛道，厂商参与度较高，来源于多个传统领域。其中，以网络安全能力为主的厂商 3 家（占比 18%），数据安全能力为主的厂商 3 家（占比 18%），应用安全和业务安全能力为主的厂商 6 家（占比 35%）。同时，专注于该赛道的新兴厂商占比也较高（占比 30%）。可见，API 安全厂商来源于多个领域，以应用安全和业务安全厂商为主，数据安全和网络安全厂商为辅。同时，作为一个新兴赛道，API 安全也吸引了众多新兴厂商积极参与。

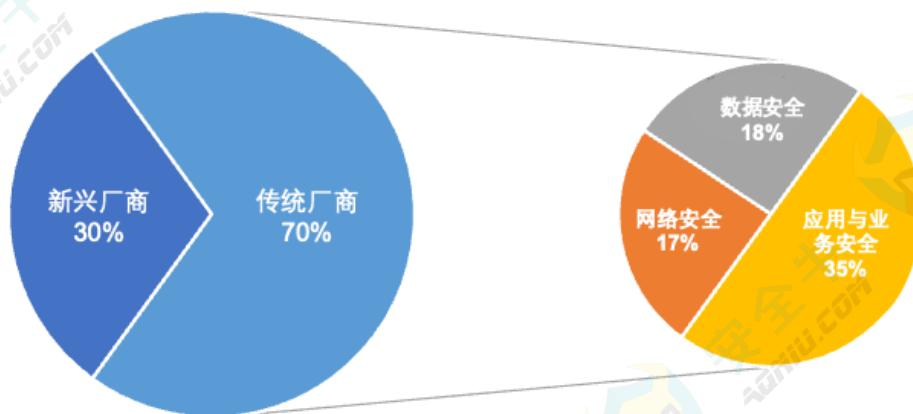


图 29 API 安全厂商类型分布

根据 API 安全评估规则，报告最后筛选了 10 家国内代表性厂商进行了能力介绍和综合评价，分别是：瑞数信息、奇安信、梆梆安全、绿盟科技、美创科技、闪捷信息、芯盾时代、安胜华信、喜数科技、安天。以下从企业介绍、产品 / 方案说明、综合评价 3 方面对 API 安全的代表性厂商能力做进一步说明

4.4.1 安胜华信

■ 企业介绍

北京安胜华信科技有限公司（简称“安胜华信”）成立于 2016 年，是一家以 API 安全为核心技术，致力于为金融、能源、运营商等关键基础行业提供服务的数字安全厂商。公司核心研发能力源自业内知名的“赛沃安全”，2018 年开始 API 安全领域的技术创新和产品迭代。技术上，坚持自主研发，在 API 参数级业务感知、广义身份识别、全应用探针、数据高速分析处理等方面有多项专利技术。结合市场需求，API 安全能力逐步与业务安全和数据安全需求融合，进一步提出了“用户 + 业务 + 数据”的业务数据安全管控理念。该公司总部位于北京，目前公司的员工人数超过 50 人，研发投入 30% 以上。

■ 方案说明

安胜华信基于 API 安全能力覆盖了“API 数据安全”和“API 业务安全”两条业务产线：

- API 数据安全 包括 API 数据安全管控平台、API 应用数据审计平台和应用数据动态脱敏网关。主要实现业务敏感数据发现、风险监测、实时管控及溯源审计。
- API 业务安全 包括一体化业务安全运营平台、API 业务安全网关和应用安全监测平台，可针对业务应用运营过程中的多源数据进行综合关联分析，实现细颗粒度的实时防护。

产品上，基于“一体化生长型”设计理念，采用统一的产品底层架构设计，通过低代码 / 无代码改动的方式，灵活配置各种安全场景防护策略，提供标准化的安全技术和服务能力。可同时满足企业互联网业务、企业内网业务以及三方 API 业务高速发展变化过程中的安全防护需求。

典型场景 包括 API 安全治理、API 数据安全、在线业务防黑灰产、全应用威胁感知等场景

行业用户 集中于金融、国央企、能源、交通行业。



图 30 安胜华信的 API 安全架构

■ 综合评价

- ① 凭借突出的创新能力，赢得了市场合作和产学研机构的认可；
- ② 拥有健全的研发管理体系，团队有较强的技术创新和工程化能力；
- ③ 方案上，紧密围绕业务和数据安全政策要求，深度挖掘行业场景化需求；
- ④ 有相对完善的 IT 运维和风险评估服务资质，可提供 API+ 数据 + 业务的特色安全运营能力。

4.4.2 安天

■ 企业介绍

安天科技集团股份有限公司（简称“安天”）是引领国内威胁检测与防御能力研究一家网络安全公司。通过 20 余年自主研发积累，安天形成了威胁检测引擎、高级威胁对抗、大规模威胁自动化分析等多方面的技术领先优势。随着威胁态势的进一步演变，2024 年推出了安天 API 雷达系统，为企业提供 API 资产和 API 相关风险管理能力。公司总部位于哈尔滨，在全国范围建有七地研发中心、九家控股子公司。目前，企业人员规模 1200 人左右，在该领域研发投入 20 人左右。

■ 方案说明

安天 API 雷达以可持续化安全防护为核心理念，通过 API 资产梳理、敏感数据识别、异常行为监测、精细策略防护等安全能力，为用户建立全面的 API 安全防御管控机制，帮助用户解决 API 资产难梳理、新型风险无有效发现手段、防护管控不知从何下手等新型业务下的各类痛点问题。相较于传统的 API 防护软硬一体产品相比，安天 API 雷达产品支持虚拟实例形态，可以在线下载、实例部署、即插即用。在简化用户部署的同时，为用户提供持续的监测和防护能力，覆盖用户 API 整个生命周期，确保 API 资产的安全性和可靠性。

典型场景 包括 API 资产梳理、API 暴露面管理、API 运行时风险监测、数据泄露监测等场景。

行业用户 主要聚焦于军工、政务、医疗、互联网行业。



图 31 安全能力框图

■ 综合评价

① 厂商具备坚实的研发基础，为其在 API 安全领域的创新提供了强有力的支持；

② 技术上融合了安天传统的 WEB 防护和威胁检测功能，同时在 API 风险识别方面又发挥了一定的创新优势；

③ 产品策略配置简单，易用性较好，支持国产化适配；

④ 服务方面，有较强的应急保障能力和服务覆盖能力。

4.4.3 楠柳安全

■ 企业介绍

北京楠柳安全科技有限公司【简称“楠柳安全”】成立于 2010 年，是一家专注于移动、物联网领域安全技术研究的网络安全公司。在技术深耕的基础上，公司建立了全面的移动应用安全防护生态体系，并在业务上形成了以移动安全为主体，联动安全服务和物联网安全的“一体两翼”业务体系，以及由技术、产品、解决方案和咨询服务构成了“四位一体”产研体系。在 API 安全方面，楠柳安全基于渠道应用黑灰产攻击趋势，及移动端新型网络攻击风险的分析，提出了端到端 & 全渠道的 API 安全防护思路，并围绕数据安全、业务安全、安全管理、事件溯源等典型应用场景，为客户提供针对性的安全方案。公司总部位于北京，在上海、深圳、广州、天津、成都等多地设有办事处，目前员工人数超过 400 人，技术团队占比超过 60%。

■ 方案说明

端到端 & 全渠道移动应用安全防护方案 核心思想是通过建设动静结合，联动不同渠道实时联防联控，实现前后端业务风险的联动机制保障业务安全运行。该方案可以重点监测人脸绕过、数据泄露、渠道洗钱、盗版仿冒、业务欺诈等黑灰产攻击，并进行此类安全事件处置、溯源，确保移动应用安全、合规运营。楠柳·API 安全平台 是该方案的核心产品，它通过对 API 上线运行后的数据流量进行实时解析及检测，识别 API 上线运行后所面临的各种安全风险，并为企业建立一套完整的 API 安全防御管控机制。功能上，通过资产管理、风险检测、敏感数据识别、脆弱性检测、风险防护管控等几大核心模块，应对资产数据难治理、风险行为难发现、数据泄露难感知、威胁攻击难防护四大安全问题。

典型场景 包括 API 安全及合规治理、API 数据防泄漏、电子渠道攻击监测溯源、反洗钱反电信诈骗、反薅羊毛及虚假营销、业务风控等。

行业用户 主要集中于金融、电子政务、互联网、运营商行业。



图 32 楠柳安全 API 安全解决方案

■ 综合评价

- ① 深耕于移动应用安全，并凭借其卓越的技术实力和专业性，赢得了客户的高度信赖和长期支持；
- ② 技术上，端 - 端分析能力与零信任理念结合，即建立了细粒度的 API 访问控制能力，同时提升了 API 资产和风险发现的精准度；
- ③ 方案方面，应用类型适配性好且全面支持国产化软硬件系统；
- ④ 服务方面，有较好的软件维护能力，及全面的安服资质、全国服务覆盖能力和应急保障能力。

4.4.4 绿盟科技

■ 企业介绍

绿盟科技集团股份有限公司【简称“绿盟科技”】成立于 2000 年 4 月，是一家致力于漏洞挖掘技术研究，并能提供优秀安全检查和评估类产品及安全运营服务的网络安全厂商。绿盟科技深耕 API 安全市场多年，配合多年的攻防实战经验，形成一套覆盖全生命周期的 API 安全解决方案。同时，不断探索 API 安全外延的应用场景与创新技术方案，力求贴近各行业实际需求，有效应对 API 带来的安全挑战。公司总部设在北京，2014 年 1 月在深圳证券交易所创业板上市。公司现有员工近 4000 人，其中研发技术人员超过 2600 人，在该领域平均研发投入 40 人左右。

■ 方案说明

绿盟科技参照国际通用 NIST 架构，遵循识别、检测、防护、响应的防护原则，推出了一套 API 安全系统化解决方案，主要包括 API 安全运营平台、API 漏洞扫描系统、API 监测与审计系统、API 应用防火墙 4 个核心产品。其中，API 安全运营平台，提供统一可视化展示平台，汇总各维度数据与事件，方便对 API 进行运营管理。该方案基于流量分析，聚焦于发现 API 自身与 API 敏感数据泄露风险，兼容个人信息保护法、数据出入境合规检测及多个行业数据分类分级规范，侧重于流动数据合规性管理与安全治理问题。

典型应用场景 包括 API 风险管理、数据出入境合规审计、数据泄露及溯源分析等场景。

行业用户 主要聚焦于运营商、金融、政务、制造业和能源行业。



图 33 绿盟 API 安全系统框图

■ 综合评价

- ① 高度注重产学研合作，积极促进网络安全前沿技术分享和交流；
- ② 技术方面，重视准确度，在资产识别和风险识别方面充分发挥了企业的技术基因优势，特别是漏洞挖掘和行为模型构建能力；
- ③ 拥有多年垂直行业深耕细作的经验，在产品中重视行业特性的功能开发；
- ④ 服务方面，拥有非常高的全国服务覆盖能力，以及专业的售后服务和专家团队，能为 API 安全落地提供高质量的运维保障和事件响应能力。

4.4.5 美创科技

■ 企业介绍

杭州美创科技股份有限公司（简称“美创科技”）成立于 2005 年，是国内较早专注于数据安全技术研究和治理服务的企业，拥有多项自主核心技术，是国家信息安全漏洞库和网络安全应急服务的重要技术支撑单位。基于韧性数据安全防护体系框架，重点布局了数据安全、运行安全、安全运维服务三大业务。为进一步解决应用 API 接口访问场景中的数据安全问题，美创科技自 2020 年开始推出 API 安全监测与访问控制系统产品。公司总部位于杭州，在全国 30 多个地区设有分支机构。目前员工规模 500+，研发投入 30% 左右。

■ 方案说明

美创科技 API 安全监测与访问控制系统（API-SMAC）聚焦于 API 接口流转安全，通过双向流量解析和轻代理技术，对通过 API 接口进行数据流转的行为进行安全监测、安全访问控制、链路追溯，旨在帮助用户构建 API 接口数据自由、安全流转的可信环境。核心功能包括：API 资产全面识别、API 访问权限管控、接口二次封装监测与控制、数据流转风险监测，在 Agent 模式下可进一步实现加密流量监测、数据流转链路测绘功能。

在此基础上，公司也进一步将 API 安全与其他数据安全能力紧耦合打造了新一代数据安全管理平台（DSC），增强其在数据流动管理方面的能力。



图 34 美创科技产品能力框图

典型场景 包括 API 集中管理、数据流转监测管控、数据共享交换态势分析等业务场景。

行业用户 主要聚焦于政务、能源、医疗、运营商行业。

■ 综合评价

- ① 产学研参与度较高，凭借 API 安全领域深耕与实践，积极推动应用接口的标准化和创新应用，多次获得权威机构认可；
- ② 技术上，接口的细粒度的访问控制与 API 风险管理能力结合，真正实现了“识别 - 防护 - 检测 - 处置”一体化；
- ③ 产品功能完善度和成熟度较高，注重友好性设计，场景应用灵活，能全面支持信创软硬件平台；
- ④ 拥有较高的运维、安全服务资质及全国服务覆盖能力。

4.4.6 瑞数信息

■ 企业介绍

瑞数信息技术（上海）有限公司【简称“瑞数信息”】成立于 2012 年，是中国动态安全技术的创新者，专注于 Bots 自动化攻击防护领域的专业解决方案。公司聚焦新一代应用安全与数据安全建设，提供全面覆盖 Web、APP、API 的全渠道应用安全、业务安全、数据安全及反勒索、数据恢复与备份等领域的产品及服务。总部位于上海，分支机构分布于全国 20 多个城市，成都、上海和北京分别设有研发中心和研发团队。目前拥有员工 300 人左右。

■ 方案说明

瑞数 API 安全解决方案包括 API 安全扫描器、WAAP 防护、API 安全审计三个产品，可以从事前、事中、事后三个环节帮助用户构建完整的 API 安全防护体系。

- **事前扫描：**事前采用 API 安全扫描器。该产品可在开发阶段对 API 安全风险的扫描和评估，使 API 资产发现手段由被动变为主动，主动实现对 API 安全漏洞和缺陷的探测。
- **事中防护：**事中采用 WAAP 防护产品。该产品可在应用运行阶段覆盖 Web、APP、小程序所有 API 接口的访问通道，通过 WAF 能力、Bot 防护能力、DDoS 防护能力和 API 管控能力，实现实时风险和攻击的全渠道防护。
- **事后审计：**API 安全审计提供事后溯源，业务深入分析能力。

典型应用场景 包括 API 资产发现与管理、API 攻击检测与防护、异常行为监控、API 访问行为审计、敏感数据管控、API 漏洞扫描、API 安全风险评估等。

行业用户 聚焦于运营商、金融、央国企、政府、能源行业。

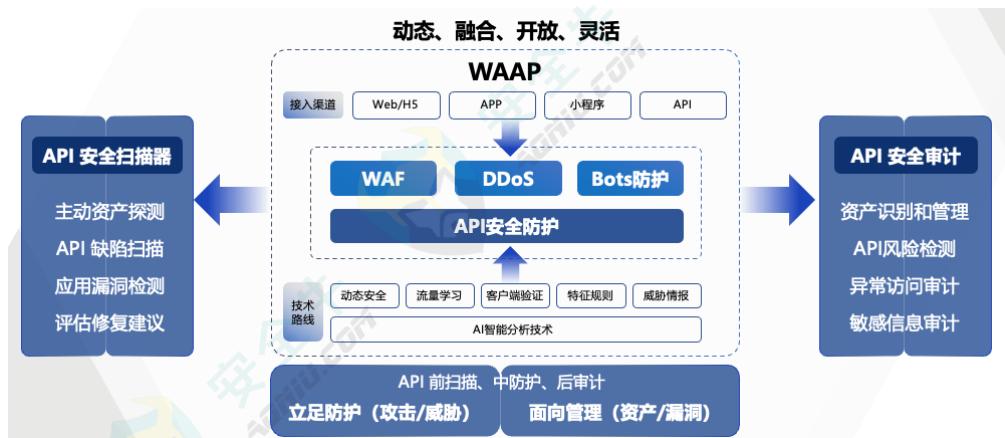


图 35 瑞数信息 API 安全能力框图

■ 综合评价

- ① 注重品牌建设和产学研合作，市场增长稳定；
- ② 技术上，创新能力表现优秀，重视应用自动化、自学习识别技术提升风险识别效率；
- ③ 产品方面，注重系统化、模块化设计和行业特性化应用，兼顾产品灵活性和专业性；
- ④ 方案上，运用安全左移（验证）和风险防护闭环的原则，实现了 API 生命周期全面覆盖；
- ⑤ 重视运维服务和应急响应服务，并具备较好的服务覆盖能力。

4.4.7 奇安信

■ 企业介绍

奇安信科技集团股份有限公司【简称“奇安信”】成立于 2014 年，是专注于网络空间安全市场，提供新一代企业级网络安全产品和服务的供应商，2020 年登陆科创板上市。持续的创新研发和实战攻防能力是奇安信的核心优势。随着技术发展，公司在安全大数据、人工智能、安全运营技术方面也逐渐形成了行业领先优势。基于对网络安全细分市场的研究，公司在 2022 年发布了 API 安全产品，并结合集团全栈的网络安全技术形成了检测、分析到数据防护的全面 API 安全解决方案。目前，API 产线由公司云和大数据安全事业部负责，BG 研发投入 80 人左右。

■ 方案说明

奇安信 API 安全卫士是针对数字化转型业务中有数据安全和 API 安全需求的产品与解决方案。该方案由 API 安全检测系统、API 安全（数据）防护系统、API 安全分析与管理平台形成一整套从发现、检测、分析、防护的闭环解决方案。通过 API 资产管理、API 风险监测、数据泄露分析、数据安全保护等技术帮助企业缩小 API 的暴露面、识别 API 潜在的风险、防止敏感数据泄露、并提供敏感数据访问的溯源手段。

典型应用场景 包括 API 资产运营、API 安全风险管理、实战攻防演练、云安全资源池化、敏感数据泄露监测等应用场景。

行业用户 主要聚焦于电子政务、金融、能源、医疗等行业。



图 36 奇安信 API 安全卫士能力框图

■ 综合评价

- ① 参与多项 API 安全赛事和行业标准化工作，积极引领 API 安全的细分赛道发展和垂直行业应用；
- ② 技术上，继承了应用资产识别和流量分析方面的技术优势，资产梳理、风险识别、风险溯源能力表现优秀；
- ③ 产品功能完善，风险分析可视化、交互设计、易用性体验较好；
- ④ 有较强的应急保障团队，支持云端 + 本地结合的安全运营模式，并提供专业级的 API 安全卫士报告分析和运营服务。

4.4.8 闪捷信息

■ 企业介绍

闪捷信息科技有限公司（Secsmart） 成立于 2015 年，是归国留学人员创办的一家专注数据安全的高新技术企业。公司创新提出了“云·管·端”立体化动态数据安全理念，实现结构化和非结构化数据资产的全面管理与防护，构建了覆盖大数据安全、云数据安全、应用数据安全、数据防泄漏、工业互联网安全、数据管理和治理等领域的全栈数据安全产品体系与服务能力。2021 年开始，基于 API 安全推出应用数据安全审计类产品。该公司总部位于杭州，全国设有 2 个研发中心和 20 多个分支机构，目前拥有员工 500 人以上。

■ 方案说明

应用（API）数据安全审计和应用（API）数据安全访问控制是闪捷应用数据安全系列的两款产品。产品围绕“发现 - 治理 - 监测 - 防护”的 API 数据安全治理思路，利用接口挖掘算法、数据识别技术和内置的脆弱性和风险检测模型，在不改造业务的前提下，一方面实现 API 接口识别和盘点、敏感数据动态识别、API 接口脆弱性检测、异常行为风险感知等实时扫描和监测；另一方面对 API 敏感数据进行接口级动态调用脱敏和数据水印标注保护，让用户 API 资产清晰可查、API 安全威胁可见、敏感数据流转可溯。该方案可以帮助用户构建从事前资产梳理到事中动态防护、事后溯源补救的 API 全栈数据安全防护体系，助力企业轻松应对复杂 API 安全挑战，实现数据与业务的双重保护。

典型应用场景 包括 API 风险监测、API 权限管控、API 数据脱敏、API 数据水印等多个场景。

行业用户 主要集中于政府、金融、互联网企业。



图 37 闪捷信息应用（API）数据安全产品能力框图

■ 综合评价

- ① 该厂商基于 API 安全持续深耕数据安全，积极参与行业的标准化工作，并有稳定的客户源和广泛的客户影响力；
- ② 技术上，有传统数据访问控制的优势，并应用 AI、大数据、自然语言学习技术持续创新，增强应用数据多维度的溯源能力；
- ③ 产品方面，分别打造审计和访问控制应对不同场景需求，产品成熟度较高；
- ④ 提供运维和风险评估服务，拥有较高的全国服务覆盖能力。

4.4.9 芯盾时代

■ 企业介绍

北京芯盾时代科技有限公司【简称“芯盾时代”】成立于 2015 年，是一家专注于零信任业务安全的网络安全厂商。公司拥有“智能业务安全”和“零信任企业安全”两大产品线，致力于为客户提供覆盖业务全生命周期的安全解决方案。围绕业务安全，芯盾时代形成统一终端安全、智能决策大脑、零信任网络访问等多项核心技术。覆盖移动办公安全、全场景统一身份管理、网络边界安全防护、用户行为风险分析、金融账户及交易安全、交易 / 信贷 / 营销风控决策和反欺诈、移动 APP 安全等应用场景。为进一步提升企业业务的安全性，2020 年开始，陆续推出 API 安全相关能力。芯盾时代总部位于北京，在全国十余地设有办事处和分支机构。目前企业员工规模近 400 人，API 研发投入近 20%。

■ 方案说明

芯盾时代 API 安全监测平台 包含 API 流量解析与管控、API 资产发现与管理、API 资产脆弱性分析、API 异常行为检测、数据安全分析等功能模块，能针对后端 API 服务的访问控制类安全需求，提供 API 接口统一代理、访问认证、数据加密、安全防护、应用审计等功能。特别是针对内网 API 资产梳理、API 接口漏洞检测、API 异常行为发现、API 接口敏感数据泄露等问题，该平台作为企业级 API 安全防护的基石，能够帮助客户提升整体的安全防护能力，保护其核心业务不受安全威胁。

典型应用场景 API（应用）资产梳理 / 画像、API 访问风险监测和审计、风控反诈等场景。

行业用户 主要聚焦于金融、政企、医疗和制造行业。



图 38 芯盾时代 API 安全方案

■ 综合评价

- ① 基于 API 安全能力，持续深耕于业务安全，进一步加强了客户信任，保持了市场持有量；
- ② 技术上，不断运用新技术和理念，持续提升访问风险管理能力；
- ③ 方案上，遵循平台化和功能模块化设计原则，提供标准化接口和协议方便第三方集成；
- ④ 服务方面，侧重于集成和运维服务，能提供专业的 API 资产梳理和风险运营保障能力。

4.4.10 喜数科技

■ 企业介绍

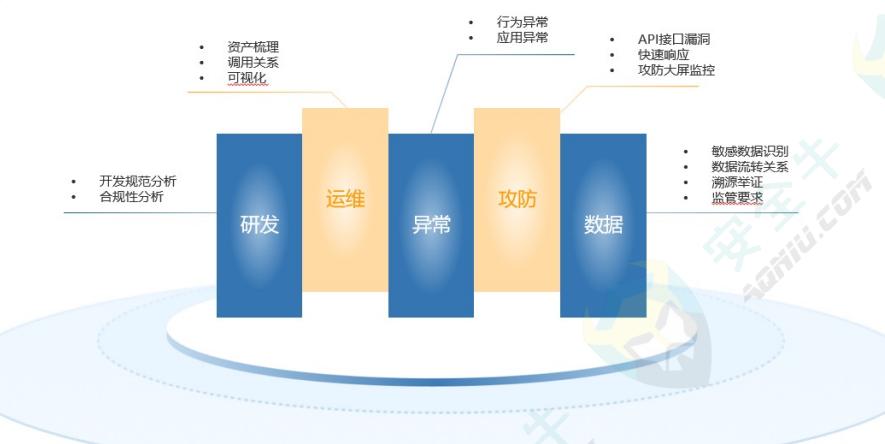
上海喜数信息科技有限公司（简称“喜数信息”）成立于 2018 年，是上海一家专业从事 API 安全技术研究开发的高科技创新企业。公司提供全面的 API 安全解决方案，推出了喜数 API 扫描器和喜数 APISEC 安全平台两大核心产品，涵盖从资产管理到实时防护的全方位服务。技术团队骨干来自亚马逊、谷歌等知名企业，具备深厚的研发创新能力。公司总部位于上海，在南京、西安和广州设有分支，现有员工人数超过 50 人，开发及服务支撑团队占比 50% 以上。

■ 方案说明

喜数信息 API 安全解决方案包括：API 扫描器、APISEC 安全平台。其中，APISEC 集风险监测和态势分析能力于一体，可以提供 API 资产管理、漏洞分析、应用分析、API 审计、数据流转分析、攻防态势展示功能。为用户打造安全、高效、合规的 API 开放平台，实现 API 安全运营闭环的落地，助力企业数字化转型。

典型应用场景 API 风险检测分析、数据流转监管、攻防演练风险监控等场景。

行业用户 聚焦于能源、金融、省市级政府、交通行业。



■ 综合评价

- ① 基于 API 安全研究在多个领域进行创新应用实践；
- ② 技术上，有一定创新能力，特别是多维度的关联分析和关系可视化，但目前风险防护方面能力有待提升；
- ③ 应用方面，可兼容传统 IT 环境和云原生环境；
- ④ 服务方面，可提供从 API 发布到运行的全方位 API 安全运维服务。

第五章 案例研究

5.1 车联网公有云环境的 API 风险监测能力建设案例

案例来源：绿盟科技集团股份有限公司

5.1.1 项目背景

随着数字化转型和大数据的重要性不断提升，API 在业务和数据架构中的应用变得越来越广泛，推动了应用服务化的显著趋势。在车联网服务行业中，API 负责应用间的数据传输和控制，在应用架构中扮演着关键角色。特别是，交通服务行业，随着国内汽车市场的快速增长和交通事故的增加得到了迅速发展。交通服务公司通过整合呼叫中心系统、GPS 定位系统、客户关系管理系统和决策支持系统，构建了高效的道路救援服务系统，以优化车主对服务资源的配置。由于业务需求，需要与汽车制造商、保险公司、金融机构的各种平台对接，存在大量的数据共享和交换需求。在行业内部，道路交通数据通过 API 接口与外部单位进行对接，这些数据传输规模大且涉及高度隐私。然而，由于合作单位的接口格式和加密方式缺乏统一标准，API 的管理变得复杂且难以统一。为了更好地保护客户和员工的个人信息安全，车联网服务行业迫切需要建立一个覆盖 API 全生命周期的安全保障机制。

本案例客户是一家科技赋能型的规模化车联网服务企业，与近 400 家主机厂、主流保险、金融、平台等企业存在业务合作。该企业通过平台以 API 接口的方式对接数百家业务单位，进行数据的接收和共享，涉及个人信息、事件数据、订单数据等多种类型。每年处理的案件数量接近千万台次，数据规模庞大且隐私性强，因此接口数据的安全性对于公司和个人都至关重要。面对大量的 API 接口和敏感数据，该企业面临着如何快速梳理历史遗留 API，并对 API 全生命周期进行安全保障的挑战。API 接口数量众多且复杂，梳理难度大，如何在实现企业系统互联互通的同时，有效保障 API 的安全性，成为保护企业整体安全并助力其数字化转型的关键问题之一。

案例中，客户希望通过构建 API 安全风险管控平台实现以下安全目标：

- (1) **API 接口管理** 识别云上应用提供的数据共享 API，特别是长期未被访问的僵尸 API，并采取下线等管控措施，以优化 API 资源的使用和管理。
- (2) **敏感数据审计** 对 API 接口中敏感数据进行审计，识别并标记重要数据和敏感数据，确保数据的安全性和合规性。
- (3) **风险审计和攻击识别** 对访问时间、接口地址、应用地址、状态码、请求方式等多个条件以审计；识别跨站脚本攻击、攻击溢出等攻击行为，提高系统的安全防护能力。

● 案例研究

(4) 事件溯源 基于 API 风险安全事件进行溯源审计，确保能够快速定位和响应安全事件，提升整体安全管理服务水平。

5.1.2 方案介绍

本方案中针对企业的 API 监测防护管理要聚焦网络中的 API 流量与敏感数据，以 API 监测管理平台为核心发现 API 自身安全风险与 API 数据泄露风险，并将 API 与数据关联起来，以数据和敏感数据为要点，提供了一整套基于 API 接口监测防护能力，对其进行 API 资产管理、API 安全风险、敏感数据识别和 API 审计溯源等安全监测服务，解决企业流动数据的分类分级与安全治理问题。系统架构如图 40 所示。



图 40 系统架构

关键技术主要包括以下三点：

(1) 多级策略逐步过滤，提高 API 资产识别准确度

API 资产识别与梳理在确保系统安全和效率方面至关重要。然而，初级的 API 台账往往存在着大量的重复 API 和噪声 API，并不方便直接使用。重复 API 可能由于参数的变化而导致 API 数量级的增加；而噪声 API 可能是由于互联网暴露面的扫描或者内网扫描，属于大量的无效 API。为解决这一问题，案例采用了多级策略逐步过滤的方法，以确保输出的 API 资产列表准确无误。首先，利用自动化的识别与优化，保持 API 资产列表的高准确性；随后，基于内容和上下文分析对 API 进行标签签注，从而进一步提升 API 安全监测能力和运营效果。这种方法不仅提高了 API 资产管理的精确度，还增强了整体安全监控的有效性。

(2) 内置敏感数据分类分级模板，提升数据合规管理能力

API 作为数据流动、共享和分发的主要载体，其安全性尤为重要，尤其是 API 传输数据的风险管理。绿盟

科技凭借多年的数据安全积累和丰富的项目实战经验，开发了一套高准确度、广泛覆盖行业的数据分类分级模板。这套模板能够精准识别数据的类别和级别。为方便数据策略配置和管理，平台系统内置了个人隐私数据模板以及3个行业分类分级模板，用于识别API传输数据的类别和级别。通过结合行业规范和实战经验的优化，该系统在敏感数据识别方面具有很高的准确率。这为API安全风险识别和数据泄露风险防范提供了坚实的基础，确保企业在数据管理和安全防护方面处于领先地位。

(3) 异常行为发现模型结合多维分析能力，提升风险识别准确性

API安全风险与传统WAF的最大区别在于API的灵活性，这使得基于特征匹配的检测方式效果有限。为弥补特征检测的不足，异常行为分析成为关键手段。API监测管理特别重视API异常行为识别的能力，并通过开创性的多维分析方法，显著提升了异常行为识别的准确度。这种多维分析方法包括数据维度、账号维度、频率维度和生命周期维度。通过综合分析这些维度，系统能够更准确地识别和响应API的异常行为。这种方法不仅提高了检测的精确性，还增强了对潜在安全威胁的预警能力，为企业提供了更为全面的API安全保障。

该用户业务系统部署在公有云的基础设施上。方案在实施过程中，采用Agent引流公有云VPC内流量到API安全监测平台，解决了公有云VPC内流量不出VPC问题；策略上，依托事件分析引擎、上下文理解引擎等能力，解决API资产管理、安全监测、数据泄露等风险问题。部署拓扑结构如图41所示。

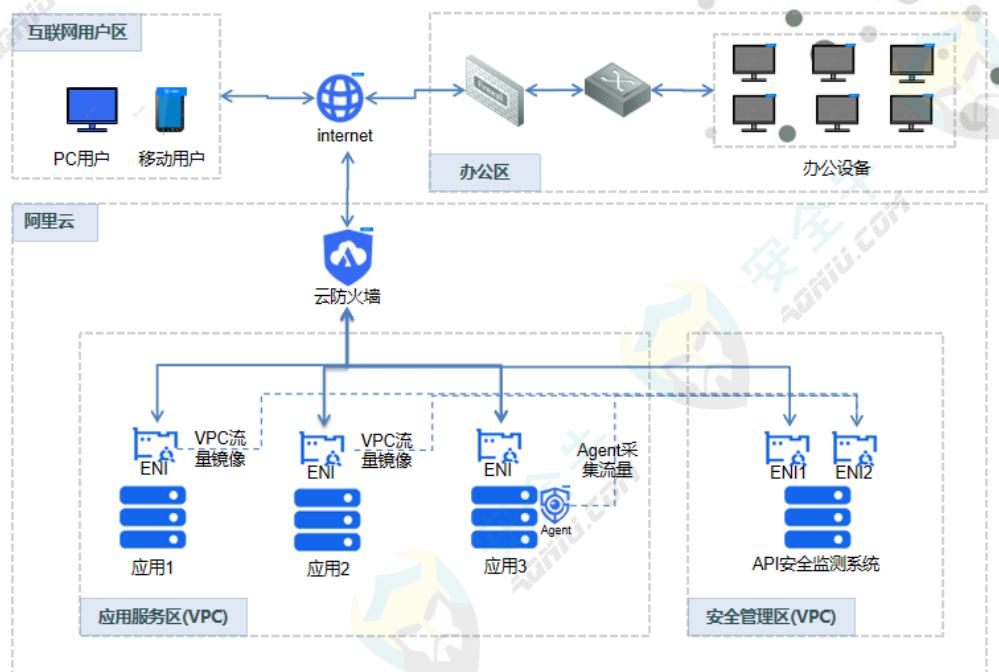


图41 方案部署图

5.1.3 方案价值

- 通过实时监控API调用情况、响应时间、数据流向及异常行为，有效保障了数据传输的安全性

● 案例研究

方案内置了个人隐私数据模板和分类分级模板，可在 API 交换敏感信息时，监测数据流量，分析访问模式和频率及时发现不寻常的流量波动和访问行为，这些通常是潜在安全威胁的早期迹象。一旦检测到异常，可以及时采取措施，如，限制访问、发送安全警报或封锁恶意流量，从而防止数据泄露或未授权访问，实时监控涉及车辆的个人信息、事件数据、订单数据的数据流转情况。因此，API 安全监测不仅是数据安全的第一道防线，也是维护系统完整性和确保敏感信息安全的关键手段。

(2) 数据流转可视化，能直观地了解系统内部及其与外部系统之间传输时的安全状况

平台对数据流转过程中的安全性进行实时可视化，使得客户能够直观地了解数据在系统内部及其与外部系统之间传输时的安全状况。这种监测不仅包括数据传输的实施情况，还涉及对潜在的安全威胁和漏洞的识别。通过图形化的界面，客户可以清晰地看到哪些数据被安全地处理和传输，哪些部分存在风险，从而及时采取措施进行防护或修复。通过明确展示数据安全流转的全过程，API 安全监测实现了数据保护的透明化，可增强客户对数据保护措施的信心，也使得客户在面对日益复杂的网络安全威胁时，能够更加有效地管理和保护其关键数据资产。

(3) 帮企业实现了内、外网高风险攻击面的梳理

API 监测管理通过建立资产基线，发现影子 API、僵尸 API，形成完善的资产列表，帮助用户识别内外网的 API 资产。同时，详细地揭示 API 的脆弱性，为用户构建了一个清晰的攻击面视图。进一步地，通过 API 监测管理的资产识别和风险检测能力，使得用户能够基于这些信息制定和实施更为针对性的安全策略和措施，有效降低风险，提升整体的安全防护水平。

(4) 提升了企业的风险防御能力和运营效率

在安全运营过程中，通过 API 风险监测，企业能够迅速发现未授权访问、数据泄露、滥用 API 的行为和其他安全威胁，精确地识别和响应安全事件，尤其是那些直接影响数据流、数据访问和应用程序功能的事件。通过集成 API 监测管理能力，安全运营团队不仅能够提升防御能力，还能够优化资源分配，通过专注于最关键的安全威胁来提升整体的运营效率。

5.1.4 案例点评

【安全牛评】该方案通过探针的方式适配云原生环境全息 API 资产监管的需求，重视运用先进的行为分析技术提升资产和风险的识别精度应对云环境的动态性和复杂性，并且紧密贴合行业数据治理的合规要求。方案从部署和检测能力上都进行了云化适配，体现了在云原生环境中应用的专业性和先进性。在不同行业的云原生安全中具有广泛的适用性，可以为希望通过 API 治理、数据合规流转监管提升云原生安全运营能力的用户提供参考。

5.2 API 安全管控系统助力电信行业网络防护的案例

案例来源：瑞数信息技术（上海）有限公司

5.2.1 项目背景

数字化时代下，API 作为连接各种应用和系统间的桥梁，已经成为企业实现业务上云、提高业务效率、拓展业务边界的重要工具之一。随着 API 的爆发式增长，攻击者也针对其开放性和普遍性的特质展开威胁和攻击，导致重大的安全隐患和数据泄露风险，对企业造成严重损失。为了应对层出不穷的新型攻击手段和各类安全挑战，企业亟须对 API 进行统一治理。

南方某省移动运营商作为中国移动的子公司，是本地通信行业的主导运营商。该公司为客户提供“全球通”“动感地带”“神州行”“集团网”客户品牌的移动通信信息业务，与上千家企业合作建设了企业信息网。随着数字化建设的不断推进，该运营商广泛应用基于 API 连接的业务，涵盖了官方网站、网上营业厅、网上商城、第三方支付、微信小程序和公众号等移动应用，极大地便利了数据的流动与交互。然而，在实际应用过程中，这种便利也使企业面临了风险管理的严重挑战：

(1) API 资产管理困难

在业务系统中，新旧业务和架构并存。同时，不同的业务系统分散在本地或云环境中不同的位置运行，难以有效跟踪。随着 API 资产的不断增长，资产梳理和管理愈发困难，企业无法清晰 API 资产的安全现状。

(2) API 敏感数据泄漏，异常调用风险大

通过 API 接口，数据信息在用户与企业之间进行流通和交互。但由于缺乏有效的监测手段，难以及时发现 API 接口在数据传输过程中是否携带敏感信息或存在异常调用的情况。

(3) API 敏感数据分级分类困难

为实现对 API 数据实现全方位的管控，必须优先解决 API 敏感数据的分类分级难题。然而，由于业务数据中敏感数据的多样性、分类标准的复杂性以及分级策略动态调整的需求，这一过程也面临诸多挑战。

(4) API 新兴威胁难以防护

API 的开放使用模式使网络边界逐渐模糊，增加了风险传导路径，扩大了网络攻击面，API 业务也逐渐沦为黑客重点攻击目标。传统的防护边界和手段难以应对当前业务模式下 API 面临的各种新兴威胁。例如，利用高级自动化工具对 API 恶意调用、通过正常业务接口实施撞库攻击和数据窃取等。

● 案例研究

5.2.2 方案介绍

根据需求，瑞数信息通过瑞数 API 安全管控方案，为用户打造了集“发现 - 检测 - 分析 - 防护”能力于一体的 API 风险管理能力。

如图 42 所示，方案以 API 资产管理为重点，以 API 安全审计为核心，帮助企业实现自动发现 API 资产、检测安全攻击、识别请求中的敏感数据、监测运行状态、审计访问行为以及识别应用缺陷等风险管理能力。该方案也进一步提供了安全审计报告，全面透视 API 数据安全的整体情况，为系统化联防联控提供支撑。



图 42 方案框图

该案例中的关键技术包括以下 4 个方面：

(1) 应用数据建模和流量分析技术进行 API 资产管理

基于数字建模技术，系统能够自动识别被保护站点的 API 资产。流量分析，自动发现流量中的 API 资产和敏感接口，并将 API 按域名进行分组管理，指派相应的责任人和部门，实现数据的分权管理。

(2) API 数据透视

通过可视化的 WEB 视图，详细展示当前 API 治理情况，透视 API 数据安全现状。包括 API 资产管理、API 安全防护、API 异常行为、API 敏感信息监测情况等。

(3) 敏感数据分级

根据运营商的行业规范，系统内置了电信行业数据分级模板。通过敏感数据自动分级、自定义敏感信息的级别，快速为不同敏感等级的数据制定适用的 API 数据安全策略。

(4) API 攻击防护

在攻击防护方面，采用了智能规则匹配及行为分析的智能威胁检测引擎，持续监控并分析流量行为，有效检测威胁攻击。同时，运用语义分析和流量学习技术，精准、快速识别各类漏洞利用、Bot 攻击行为，对 API 请求参数和逻辑调用顺序进行检测，有效应对诸如爬虫、撞库等各类针对 API 的威胁。

该案例中业务系统部署在传统 IT 系统环境中。API 安全管控系统在部署中，采用了南北向反向代理模式，并采用了集群模式实现高可用性。

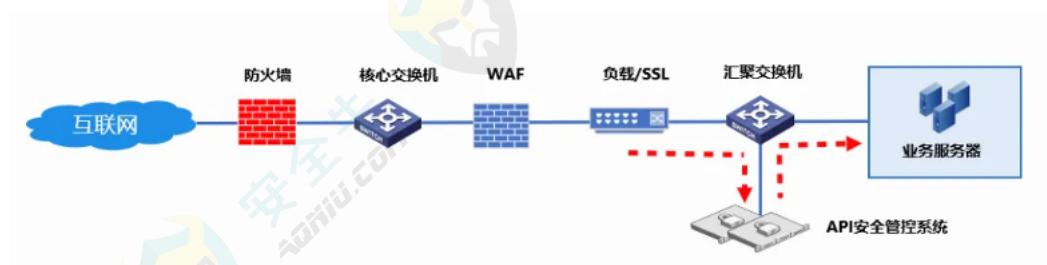


图 43 部署拓扑

5.2.3 方案价值

防护期间，API 安全管控系统梳理并确认 1500 多个 API 资产。其中，被攻击资产 730 多个，发现攻击事件 4800 多起。数据安全管理方面，识别到 400 多个资产存在敏感数据，敏感资产占比达到 26.6%。

该方案在为企业提供应用价值的同时，也为企业提供了如下两个创新点：

(1) 全方位的威胁发现和自我提升告警准确性的能力

系统通过预置的 20 多种常用的业务威胁模型和违规记录进行训练，同时结合随机采集的信息组合建模，可以同时检测已知违规行为和未知异常行为，识别或阻拦绝大多数批量恶意请求，实现对异常行为的全面监测，告警准确率达到 80%，并具备自我提升告警准确性的能力。

(2) 先进的敏感特征识别能力

采用机器学习和 AI 判断算法，结合多种类的敏感数据识别策略，能够全面覆盖运营商行业几十种常见敏感数据类型。针对不同业务的特点，提供自定义标签功能，让敏感数据的识别更加精准和贴合实际需求。

5.2.4 案例点评

【安全牛点评】 该方案采用了反向代理的部署模式，实现了“发现 - 检测 - 分析 - 防护”一体化。注重访问控制和风险防护能力结合、先进的智能化防护技术应用及行业特性的融合，充分体现了全方位、集中化、细粒度的访问控制管理能力。是南北向 API 网络访问控制的典型应用方案，值得借鉴和推广。

5.3 金融行业云原生 API 安全体系建设案例

案例来源：奇安信科技股份有限公司

5.3.1 项目背景

近年来，随着金融科技的快速发展，API 已成为金融行业不可或缺的技术基础设施。然而，API 的广泛应用也带来了新的安全挑战。为了应对这些挑战，监管机构相继出台了一系列规范和要求，以加强金融行业 API 安全建设。特别是《关于金融行业标准加强商业银行应用程序接口安全管理的通知》和《关于系统查询漏洞导致客户信息泄露风险的提示通知》分别从安全要求和风险排查两个方面提出了 API 安全要求。在监管政策的推动下，金融行业 API 安全建设成为一项重要而紧迫的任务。

某银行在数字化转型的大背景下，积极构建金融操作系统（云原生场景），不仅实现内部服务的高效运作，还积极连接外部服务，将金融操作系统从内部企业级向跨界生态级延伸。该机构的业务系统采用微服务架构，部署涉及 200 多个容器节点，服务之间通过 API 进行数据传输，东西向和南北向流量总和达到 30Gbps。面对如此复杂的系统架构和高流量环境，该银行在 API 安全建设方面面临以下三大痛点：

- (1) 监管合规风险：金融监督管理总局定期扫描暴露在互联网侧的 API 接口，以发现潜在的安全风险。该银行担心因 API 安全问题而被监管单位通报，这成为当前亟须解决的主要痛点。
- (2) 敏感数据泄露风险：特别是在 HW 活动中，担心 API 接口遭受攻击，并导致敏感数据泄露。如何快速发现并处置异常复活的 API 接口，以及有效防止敏感数据泄露，是该行面临的另一个主要挑战。
- (3) 商誉和经济损失风险：银行对外暴露了大量 API 接口，如果因 API 安全问题导致客户信息泄露或服务中断，不仅会影响银行的商誉，还可能带来严重的经济损失。

为了应对以上痛点，该银行依照云原生技术架构模型及业务开放模式，制订了以下 API 安全建设目标：

- (1) 针对云原生对外服务模式，建设强大的 API 安全防护能力；
- (2) 针对云原生内部微服务之间的业务调度模型，建设全面的 API 安全检测能力；
- (3) 基于云原生 API 全生命周期安全管理理念，建设统一、高效的 API 安全运营管理平台。

5.3.2 方案介绍

根据用户需求和云原生环境的特点，奇安信采用“发现 - 检测 - 分析 - 响应”的方法论，构建一套闭环的、持续监测和响应的 API 安全监测体系。该体系由三个核心组件组成：

(1) API 安全引流插件 该组件对 API 资产进行识别，实时检测 API 攻击行为和敏感数据传输情况。同时，将检测到的告警信息和审计日志实时上报至 API 安全检测分析系统。

(2) API 安全检测系统 对来自引流插件的流量采用 API 资产识别、API 漏洞攻击检测、API 敏感数据泄漏检测、API 行为审计的技术进行检测，生成 API 资产识别日志、API 业务流量日志和 API 威胁告警日志及敏感数据传输告警日志上传至 API 安全分析与管理平台进行大数据关联分析。

(3) API 安全分析与管理系统 实现针对 API 安全检测系统和 API 防护系统的集中管理能力。同时，采集 API 安全检测系统上传的 API 资产识别日志、API 业务流量日志及 API 告警日志，运用大数据关联分析技术进行 API 暴露面的梳理、API 威胁事件、API 敏感数据泄露事件的归并能力以及 API 异常行为的发现。

方案采用了 API 资产识别、API 资产打标、API 资产聚合、攻击威胁检测、敏感数据传输检测、异常行为分析等技术。能有效针对 API 全生命周期进行监控，识别出活跃、失活、复活、僵尸、已下线的资产。此外，还引入了专注于监测失活转复活的 API 监控机制，能够智能判断 API 接口的复活是正常行为还是异常行为。

为进一步构筑了全方位的 API 安全防护体系，项目实施中部署了相关策略使 API 安全管理系统实时监测容器云环境中的东西向流量，精准识别潜在风险和隐患；将全量的网络行为数据都以标准化格式存储在 API 安全管理平台中，便于后续分析和审计。此外，在闭环管理方面，针对外部攻击威胁，系统以告警和 API 安全事件的方式实时推送至日志服务器和 SOC 运营管理平台，实现安全事件的集中管理和响应；对于软件自身缺陷，利用工单系统反馈至开发侧，完成软件缺陷整改。拓扑如图 44 所示。

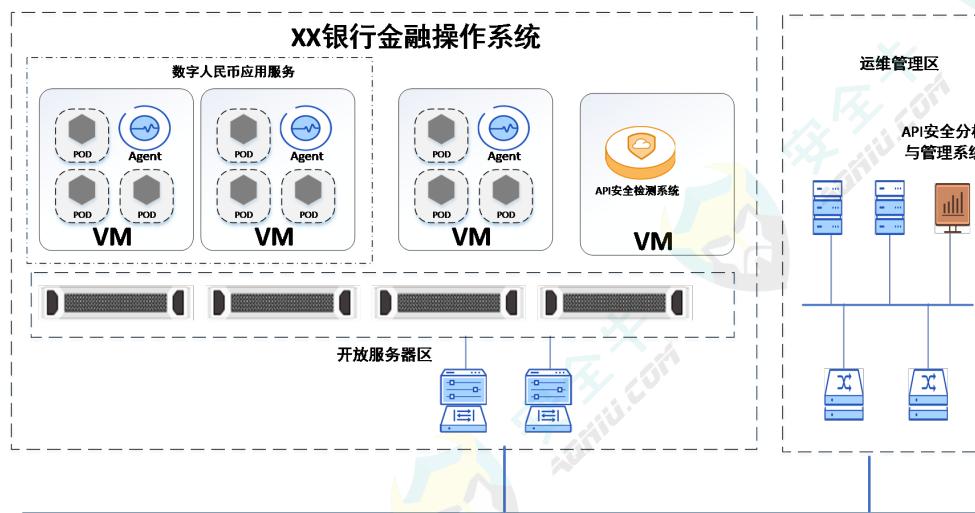


图 44 部署拓扑示意图

项目建设中，部署了一套功能强大的 API 安全管理平台，配合 6 套可容器化部署的 API 安全检测分析系统，以及 200 个与管理平台无缝对接的 API 安全引流节点。由于云原生环境的复杂性，管理平台采用物理机部署在运维管理区域，提升上线速度与稳定性；检测分析系统以虚拟化方式部署在云宏信创云，做到对业务影响最小；API 引流节点部署在信创物理机，与容器解耦。

● 案例研究

5.3.3 方案价值

首先，方案帮助用户构建了 API 资产全景图，清晰地梳理了内网和外网访问的 API，减少企业 API 的暴露。显著降低用户被监管部门通报的风险，保障了企业的合规性和声誉。

其次，方案为用户提供了针对僵尸 API 异常复活的监控能力。一旦发现因攻击或异常访问而复活的 API，系统会立即发出警报，提醒用户及时处置。这一功能可以有效防止敏感数据泄露的情况发生，为企业的数据安全提供了坚实的保障。

最后，方案帮助用户构建了整体的 API 安全防护体系，实现了 API 安全左移和风险闭环的目标。通过将安全措施前移到开发阶段，并建立起完善的风险响应机制，用户可以最大限度地降低 API 安全风险，提升整体安全水平。

5.3.4 案例点评

【安全牛点评】该方案通过可分布部署的组件为云计算系统构建了一个 API 资产安全集中监管的体系，同时遵循了安全一体化建设的思想，联动云安全运营平台实现了集中的风险防护和闭环处置。方案注重 API 资产梳理及其活动状态的管理，建设中不仅考虑了安全组件在云环境中的适配性，还充分运用了云原生的资源优势对 API 安全监管体系进行云原生化改造，提升方案的可扩展性、性能和可用性，满足云上 API 不断扩增的监管需求。

5.4 API 安全监测系统助力医疗企业数据安全防护的案例

案例来源：北京芯盾时代科技有限公司

5.4.1 项目背景

随着数字化时代的到来，API 应用日益广泛。但因其携带大量敏感数据，也带来了安全性风险、数据隐私问题。为应对这一挑战，国家出台了《数据安全法》《个人信息保护法》等法律法规要求企业在数据处理活动中加强风险监测工作，及时判定企业的 API 是否存在风险。

医疗行业是一个业务系统高度复杂的领域。某三甲医院在智慧医院的转型过程中，医院引入了大量的在线业务系统，如电子病历、体检系统、在线挂号、电子化平台等。根据智慧医院建设标准，这些系统需要实现互联互通提高医疗服务的效率和质量。然而，这也意味着不仅会有更多的 API 接口数据暴露到互联网中，并且与传统数据中心的单点调用相比，东西向接口和南北向接口的开放也导致攻击面进一步扩大。为保护患者隐私和医疗数据安全，医院亟需加强 API 安全建设。建设难点包括：

- (1) API 资产梳理难 医院老旧医疗设备众多，业务流量巨大，并且历史系统缺乏管理、跨院区安全防护难以协同，API 资产难以梳理全面。
- (2) 漏洞风险防护难 API 中存有大量的漏洞隐患，每个漏洞都有可能被黑客利用导致系统瘫痪，但医院内部系统复杂，东西向接口和南北向接口的数量巨大。传统防护能力难以应对 API 接口的漏洞风险。
- (3) 数据泄露防护难 医疗数据涉及大量的患者隐私，企业缺少敏感数据防泄漏和安全防护能力。

5.4.2 方案介绍

针对该三甲医院所面临问题，芯盾时代基于 API 安全监测系统构建了一套面向医疗行业的 API 安全防护解决方案。该方案依据《网络安全法》《数据安全法》《个人信息保护法》《关键信息基础设施安全保护条例》等法律法规，以及医疗行业的《医疗卫生机构网络安全管理办法》《医院智慧管理分级评估标准体系》等要求。

如下图所示。方案运用了大数据处理的系统架构，保证其能拥有高性能流量解析能力、高精度 API 资产识别能力、高覆盖度安全风险识别能力，满足医院巨大业务流量环境下的数据安全风险识别和威胁分析工作。该架构包括流量获取、数据预处理、业务数据缓存、流量分析、资产分析、安全分析、安全配置管理等核心模块。

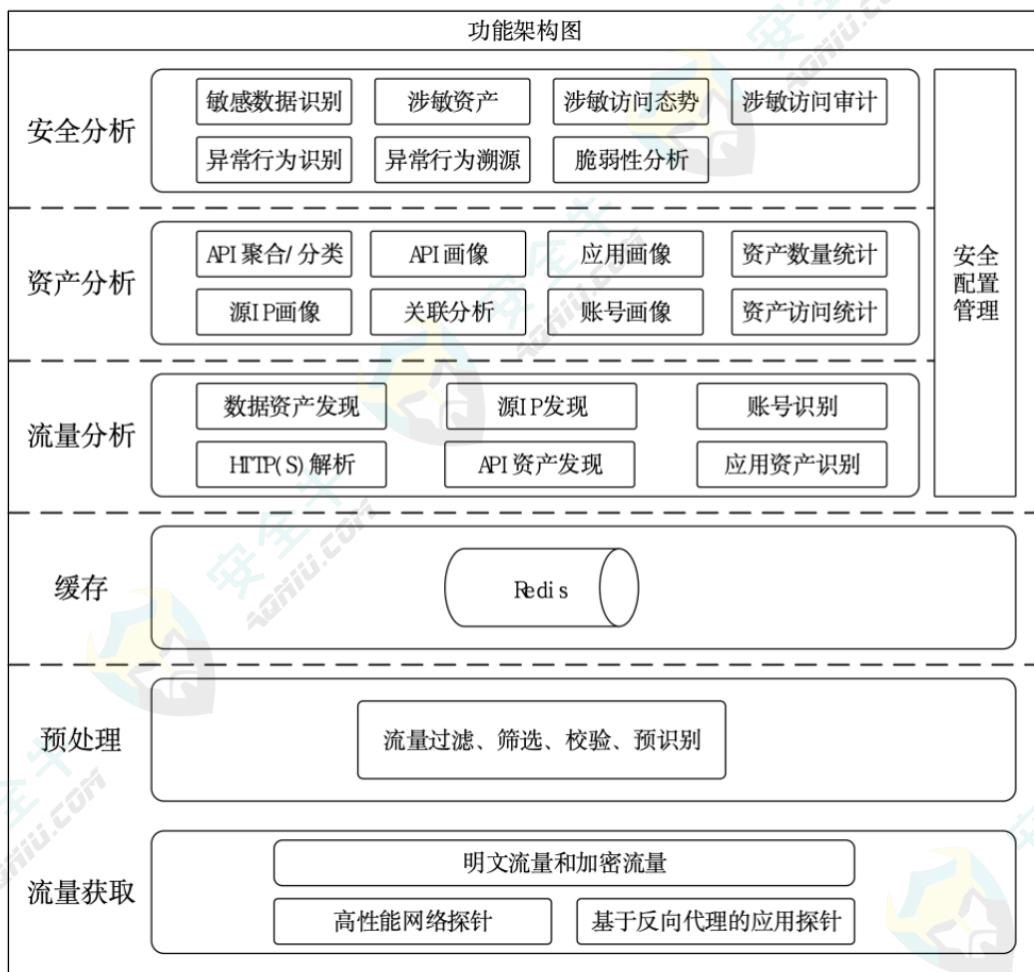
● 案例研究


图 45 系统架构

方案在资产梳理、漏洞管理、攻击监测和敏感数据识别方面的技术特点，如下：

(1) API 资产梳理方面 API 安全平台能够基于结合机器学习的 API 流量基线与自主研发的划分引擎，自动、持续发现 API 资产，对 API 进行分类，以功能、应用等多种维度聚合同类 API，形成分类明确、路径清晰的 API 资产树，让企业的 API 资产各归其类，一眼即明。平台支持多文件导入，便于新应用、新版本 API 资源的快速上传，与 API 自动发现形成互补，让企业的 API 资产管理更规范。

(2) API 漏洞管理方面 基于丰富的 API 漏洞库，API 安全平台能够自动检测 API 安全漏洞，对漏洞进行分析、定级，给出可行的漏洞修补方案，实现对漏洞的闭环管理。借助漏洞检测功能，企业可以未雨绸缪，按照先高风险等级、后低风险等级的次序修补漏洞，降低被攻击的可能性。平台支持 OWASP API TOP 10，以及 Web 漏洞的检测，支持漏洞库的持续升级。

(3) API 攻击监测方面 API 安全平台能够实时监控 API 访问情况，分析流量数据，通过内置的 API 威胁模型识别账号暴力破解、未授权访问等风险行为，通过机器学习技术对攻击进行建模、学习，持续扩展对攻击

行为的检测能力，智能识别更多种针对 API 的新型攻击，精准地发出攻击报警。安全人员可借助平台对攻击进行分析、溯源，实现对 API 风险行为的全生命周期管理。

(4) 敏感数据感知方面 API 安全平台内置敏感数据检测引擎，覆盖姓名、手机号、身份证件、银行卡号等敏感数据类型。安全人员可自定义敏感数据识别规则，实时洞察 API 接口中双向传输的敏感数据，并及时对报文中的敏感数据进行脱敏处理。平台支持对敏感事件的访问取证，安全人员可对敏感数据进行追踪溯源，提升对数据的管控能力。

项目建设分为两个阶段：

第一阶段，通过基础设施搭建和系统对接，构建系统运行环境并开展安全分析工作。在医院工作人员配合下将探针部署在网络拓扑关键节点上，完成流量接入。同时，针对医院网络实际情况调整资产解析、发现策略，更新安全策略和防护配置，保障业务分析的有效性。

第二阶段，根据用户反馈、系统运行状况进行系统优化、模型调优和功能升级。系统稳定运行一段时间后，芯盾时代派出安全分析专家和研发工程师对系统数据进行分析，调整资产发现策略、异常行为分析模型、风险识别模型，对于所发现的上百起风险事件进行处置和上报，协助该医院进行漏洞修复和问题排查。

在后期维护阶段，按照合同约定，芯盾时代公司定期派安全专家和研发工程师为用户进行系统调优、策略优化、异常问题修复，并协助进行威胁分析与安全监测。对期间发现多起安全攻击和数据泄露事件，进行处置或修补漏洞。

5.4.3 方案价值

(1) 海量流量下高精度 API 资产梳理能力

针对海量流量解析需求，通过自主研发的高性能网络探针技术，实现了对捕获网络流量的快速解析和精准分析。采用自适应的 API 接口地址聚合和智能应用识别算法，支持多种接口协议类型，具备自动发现与动态管理 API 资产的能力。特别是在应对陈旧系统遗留的 API 资产问题上，该技术能够全面梳理和整合历史遗留的 API 资产，为后续的安全管控、风险治理及运营优化提供了精准而可靠的数据支持。

(2) 强大的 API 资产行为监测和风险识别能力

系统内置超过千种 API 脆弱性识别策略，融合了调用地址、参数的语义与结构信息，以及调用行为序列特征，通过生成对抗网络（GAN）数据增强技术与图对比学习（GCL）算法的深度结合，显著提高了异常识别的精度和适应性。依托高质量高时效威胁情报，能够精准定位 API 资产中的安全薄弱环节，识别复杂场景中的潜在风险，确保企业 API 资产在安全性、合规性上的持续优化与强化。

● 案例研究

(3) 实时 API 资产安全监测与合规审计能力

系统引入图自编码器（GAE）算法对 API 调用行为进行低维嵌入表示，确保系统能够快速、精确地捕捉敏感访问和异常访问行为。结合弱监督对比学习（WCL）模型，系统能够有效识别数十种异常访问模式及敏感数据传输类型，为该医院提供全面且高效的安全态势感知能力。同时，支持细粒度的合规审计要求，保障 API 资产在各类复杂业务场景下的合法合规性。

5.4.4 案例点评

【安全牛评】 方案重视运营专家的作用，采用了 API 系统建设和 API 安全运营同步落地的模式。也让我们进一步意识到，API 安全建设是一个持续的过程，仅仅依靠系统的落地是远远不够的，持续的安全运营才是保障 API 安全的关键。这种模式不仅适用于医疗行业，也为其他行业的 API 安全建设提供了很好的参考和借鉴。

5.5 移动应用环境的 API 安全能力建设案例

案例来源：北京安胜华信科技有限公司

5.5.1 项目背景

随着移动互联网的快速发展，移动应用（APP）已成为企业开展业务的重要渠道。电力公司在电力缴费方面也在不断创新，开发各种移动应用缴费业务，给用电用户提供更好的服务体验。例如，电力公司 APP 缴费、微信缴费、支付宝缴费、银行代扣缴费等。由于电力缴费业务涉及用户信息和资金交易等高价值数据，多样化的缴费方式也给客户带来了各种新的安全风险，包括：

（1）业务前端攻击风险

近年来市场上出现了针对移动应用的各种高级逆向工程技术，如：自动化脱壳、定制 ROM、框架软件、Hook 攻击等，正在使原有的安全加固防护手段失效，导致 APP 关键业务逻辑代码泄露。进而，攻击者通过代码逻辑分析挖掘到可利用的业务逻辑漏洞，就可能攻击充电业务、盗取用户数据；或者重新二次打包一个假冒的 APP，发布到互联网上，给用户造成较大的影响。

（2）交易业务篡改风险

该移动应用中存在资金交易业务，容易遭受网络攻击、用户账户被盗刷、交易金额被篡改，给个人及公司的都带来了较大的损失。

（3）业务欺诈风险

为了推广公司业务，缴费业务场景中也会出一些营销活动，发放一些优惠券、积分奖励等等。这部分活动经常会遭到黑灰产团伙的攻击，将原本给到真实用户的福利以薅羊毛的形式获取走。

（4）充值缴费接口业务逻辑被利用风险

在移动应用的设计中，用户身份验证与关键业务操作（如充值缴费）的接口必须紧密关联，形成完整的安全闭环。但如果用户身份验证与充值缴费的接口脱节，并且认为用户认证通过后，就无需对充值缴费的接口再次进行认证，即充值缴费的接口中并未带有用户认证成功后的权限认证信息（未鉴权），充值缴费的接口就可直接被黑灰产利用，作为其洗钱的手段。

然而，传统的安全防护手段难以有效应对移动互联网环境下电力公司面向移动端、API 接口开放缴费的业务模式以及各种优惠促销的缴费场景，亟须建设专业的 API 业务安全防护能力。

● 案例研究

5.5.2 方案介绍

安胜华信基于自身的技术优势，通过 API 业务安全平台搭建数据分析的底座平台，建设了一套“安全工具 + 安全运营 + 安全管理”三位一体、互为支撑的业务安全风险运营体系。

API 业务安全平台，汇聚了终端运行数据、业务流量数据，进而针对不同的业务形态进行综合分析，为整体安全监测提供细颗粒度的分析依据。同时，采用可信识别（终端、业务、数据等安全要素的）和建模技术构建场景化的业务访问逻辑，形成从前端用户到数据及业务处理的全链路安全分析能力。



图 46 平台系统框图

该平台包括四个核心能力：

(1) 客户端风险采集

在应用客户端，集成小程序 /H5 前端 SDK。通过 SDK 可以生成唯一设备指纹信息，识别访问终端唯一设备，采集终端运行环境数据，监测客户端的运行环境风险，如：使用 ROOT 设备、使用代理访问、代码被调试分析等攻击风险。

(2) 异常访问行为分析

在业务后台，通过分析业务流量，监测访问异常的业务请求，如：越权访问，认证业务逻辑被绕过，充值缴费行为异常，业务访问序列异常等，实时发现安全风险。

(3) 业务风险模型构建

通过 API 平台自定义缴费的业务场景，对 API 的接口进行业务场景关联和链路分析，建立充值洗钱账户的

风险模型：如调用缴费接口前必须完成用户认证并且接口响应结果为成功、缴费 API 必须带有认证权限信息、同一账户短时间内多次小额为多个用户充值等风险模型，通过自定义规则模型的建立，及时识别和防范黑灰产利用缴费 API 完成资金洗白的风险。

(4) 平台化风险管理

通过平台构建技术工具，为数据识别、终端识别、风险分析，风险处置提供基础工具；从运营的角度定义资产、定义业务、分析风险，从设备、IP、用户等不同身份维度分析不同场景中涉及的业务安全风险；从管理的角度对运行状态的管控、业务的管控、合规的定义、风险的定义提供上层支撑。通过运营机制对风险模型不断优化，对已有数据进行风险数据挖掘，风险模型优化，建立长期的风险运营闭环处置机制。

该项目需要前后端同步部署以全面收集风险数据。实施中，采用了分布式采集，统一管理的部署模式。整个建设过程分为两个阶段：第一阶段，部署旁路分析能力，实现风险识别和风险监测；第二阶段，在风险监测基础上，实现 API 风险阻断。目前第一阶段已经建设完成，第二阶段正处于规划当中。

（一）前端部署，主要在应用软件客户端嵌入 SDK 探针的方式采集客户端的环境风险。

（二）后端部署，是在后端服务器机房以旁路部署 API 业务安全平台的方式采集 API 访问流量。在现场，用户业务系统分布在 3 个不同的机房。结合机房环境和业务分布情况，在互联网大区，采用了 4 台标准信创服务器来部署 API 业务安全平台，然后通过交换机镜像方式将分布的业务流量牵引到平台。

策略实施过程中，为保障项目稳妥推进，分成数据安全和业务安全 2 个步骤逐步实施。

第一步：基于 API 安全构建数据安全能力。通过资产梳理，API 弱点发现及闭环整改，敏感数据流动监测，敏感信息泄露风险发现功能，建立常态化精准告警机制。最终形成 API 资产台账，API 弱点整改台账，敏感信息流动台账，以及敏感信息泄露告警规则。其中，敏感信息泄露告警规则需要运营人员的精细化运营，逐步精确。告警量由前期的一天几千条下降到一百条以内，并且 80% 以上属于有效告警，运营人员的平均运营时间由前期的每天 4 小时以上下降到 1 小时以内。

第二步：基于 API 安全构建业务安全能力。API 业务安全平台在业务风险识别时，结合了镜像访问流量和 SDK 探针从客户端采集的设备信息及环境风险信息，进而通过关联数据分析建立多样化的业务风险模型。通过前期的精细化运营，最终形成了多个场景化业务安全风险模型，和常态化有效告警规则及运营机制，运营人员平均每天的处理时间控制在半小时以内。

● 案例研究

5.5.3 方案价值

(1) 提供了全渠道应用前端的风险感知能力

通过全应用探针技术，实现全渠道应用前端风险感知。能够实时感知 H5，公众号，小程序，Web 应用等全应用形态面临的安全风险，及时发现如手机 Root，越狱，模拟器，自动化浏览器，网络代理，恶意插件等恶意访问行为；同时具备前端设备标识能力，结合网络身份以及用户身份，解决 API 访问身份识别难题，为细粒度 API 防护创造必要条件。

(2) 实现了业务层面的 API 资产管理能力

通过自动化技术手段，对在线业务 API 进行全面资产梳理，根据其运行时参数及业务数据敏感度定义 API 属性，标记 API 所属的系统、网络，终端环境、业务类型、内部 / 外部 API 等，对 API 进行自动化分类和标签化管理。

API 资产梳理是 API 安全建设的第一步，是 API 运行时安全防护的基础。同时通过 API 梳理，能够发现有漏洞的 API，提供整改建议，不能及时整改的，制定重点防护策略。

(3) 建立了运行时的访问风险监控能力

建立 API 运行安全基线，从设备，网络，用户以及访问参数各个维度对含敏感信息的 API 进行运行时风险监控，形成有效告警机制，建立细粒度防护策略，防止数据泄漏。

5.5.4 案例点评

【安全牛点评】 该方案侧重移动 APP 环境中 API 资产安全管理，并结合了 API 风险、数据风险和业务风险的特征，提出“三位一体”的业务风险运营理念。方案注重场景化风险特征挖掘和创新型风险分析方法应用，是移动 APP 交易场景下 API 安全的典型解决方案。对保障移动 APP 的业务安全和数据安全具有重要的借鉴意义。

第六章 新兴技术对 API 安全的影响

目前阶段，尽管市场上 API 安全方案不断地推陈出新，但 API 安全的市场模式仍处于探索阶段。在建设中，识别、检测、防护等核心能力仍然面临不同程度的技术挑战，风险处置自动化能力也有待提升。

从 API 技术成熟度演进的视角来看，安全牛认为零信任、人工智能、大数据，以及云计算四类新兴技术在快速发展的同时也将会进一步赋能 API 安全，并在提升 API 风险检测的精准度、覆盖度和自动化防护处置能力方面提供助力。



图 47 对 API 有显著影响的新兴技术

6.1 零信任技术

零信任“从不信任，始终验证”的数据安全访问理念，也是 API 安全的重要思想。基于零信任理念的身份为中心、持续验证、权限最小化、动态访问控制、数据加密等技术，都将显著提升 API 访问过程中身份验证和授权的严格程度，实现更精细化的风险管控，有助于 API 网关类产品更有效地应对 OWASP TOP10 列举的各种 API 风险，满足数据安全领域日益提高的精细化防护控制要求。

此外，零信任安全强调持续的安全监测和风险评估。对 API 的调用情况需要实时监控，及时发现异常行为和潜在威胁。这就要求 API 安全策略的自动化配置和管理，减少人工干预，提高安全响应速度。同时，API 安全还需要与身份管理、威胁情报、安全分析等系统紧密集成，共享安全上下文，实现全面防护。

总之，零信任安全理念推动企业重新审视和设计 API 安全架构，从传统的边界防护转向更全面的纵深防御。企业需要运用零信任理念升级 API 安全策略和技术，提高 API 安全的严格性、精细度、自动化和智能化水平，以适应日益严格的零信任安全环境需求。

6.2 人工智能（AI）和机器学习（ML）

API 风险特征复杂并且夹杂了很多新型攻击手段，传统的基于规则的安全检测方法会产生大量漏报，难以全面识别各类 API 风险。需要大量依赖语义分析、行为分析、风险建模等新型检测技术，AI 和 ML 在这些方面发挥了重要的作用。

AI 和 ML 通过对 API 调用模式的学习，可以建立正常行为基线，及时发现潜在的 API 滥用和攻击；通过学习用户的正常行为，识别出异常用户活动，自动化攻击行为等，从而实现更精准的风险控制。ML 根据多维度的数据，如 API 调用参数、用户属性、设备信息等，对每个 API 请求进行实时风险评分，发现新的威胁模式，如新型的 API 攻击手法，帮助企业快速响应新出现的安全威胁。此外，AI 和 ML 还可以通过分析 API 的设计、实现和使用模式，自动发现潜在的安全漏洞，如未授权访问、数据泄露等。这可以帮助企业在 API 开发和部署过程中及早发现和修复安全问题。

语义分析、行为分析、风险建模等方面的能力等新型检测技术弥补了传统规则检测的不足，提供了更全面、更智能、更精准的 API 安全检测能力。更有效地帮助企业应对 API 风险特征的复杂性和多样性。将 AI 和 ML 技术与 API 安全深度融合，将成为企业有效管理 API 风险的关键举措。

6.3 大数据技术

随着 API 的广泛应用，API 调用产生的数据量呈爆炸式增长。传统的安全分析方法难以有效处理如此庞大的数据规模。大数据分析技术凭借其处理海量异构数据的能力，在数据处理、复杂关联分析、用户行为分析、异常检测、风险预测、安全态势感知等方面显著提升 API 安全的全面性、精准性和智能化水平。

企业应积极采用大数据分析技术，构建 API 安全大数据平台，挖掘安全数据价值，实现对 API 安全的全方位感知和防护。

6.4 云计算和容器化技术

云计算和容器化技术的发展给 API 安全带来了新的机遇和挑战。

随着企业应用向云端迁移，云原生 API 安全能力变得越来越重要，云原生 API 安全需要考虑 API 的云端暴露、多租户隔离、动态调度等特性，提供与云环境深度集成的安全解决方案。容器化环境下，需要重点关注容器间

API 通信安全、细粒度访问控制、服务网格安全和 API 可观测性等方面。同时，服务网格等新兴技术也为微服务架构下的 API 安全提供了新的解决方案，如通过 sidecar 代理拦截微服务间的 API 调用，为应用层 API 提供统一、一致的安全保护。

这要求企业需要采用云原生安全最佳实践，积极拥抱服务网格等创新技术，构建全方位的 API 安全防护体系。

参考资料

- 【1】 国家标准委 .GB/T 35273-2020 信息安全技术 个人信息安全规范 .2020-03-06
- 【2】 工业和信息化部 .YDT 4248-2023 电信网和互联网 API 数据安全技术要求和测试方法 .
- 【3】 中国人民银行 .JRT0185-2020 商业银行应用程序接口安全管理规范 .2020-02-13
- 【4】 李鑫 .《微服务治理：体系、架构及实践》. 北京：电子工业出版社 .2020-05
- 【5】 OWASP 基金会 .OWASP 安全编码规范快速参考指南 .2010
- 【6】 Forrester. The Eight Components of API Security.2023-09-23
- 【7】 Gartner. Hype Cycle for Application Security.2024
- 【8】 <https://www.nylas.com/api-guide/>
- 【9】 <https://api.gov.au/sections/api-security.html>
- 【10】 <https://swagger.io/specification/>



扫码开启报告AI互动

零时代·安全牛

网络安全旗舰智库



欢迎关注安全牛