数世咨询
Digital World Consulting

API 安全市场指南

2024

© 北京数字世界咨询有限公司 2024.3

数世咨询
Digital World Consulting

API 安全市场指南

2024

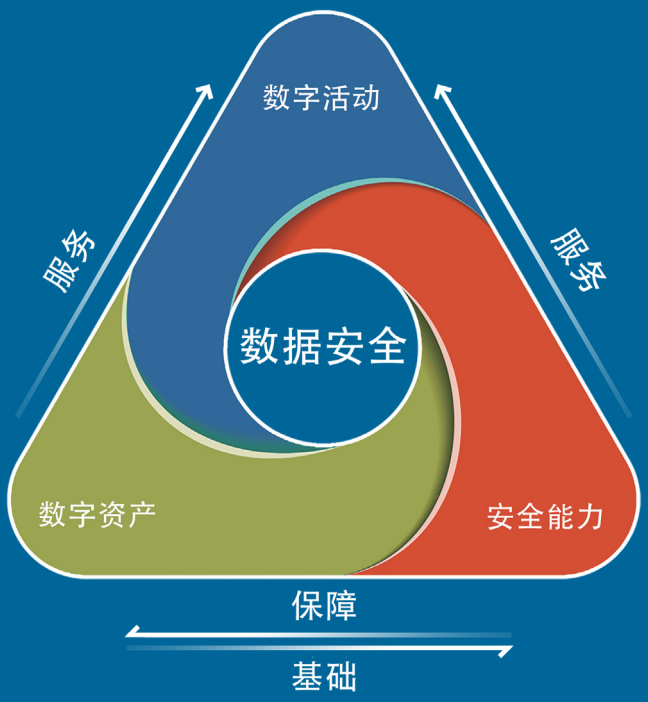
© 北京数字世界咨询有限公司 2024.3

数字安全是指，在全球数字化背景下，合理控制个人、组织、国家在各种活动中面临的数字风险，保障数字社会可持续发展 * 的政策法规、管理措施、技术方法等安全手段的总和。

这里的风险，不再局限于围绕数字化资产的攻防对抗，还包括了数字资产所承载业务的稳定性、连续性和健康性。这里的安全不再特指有意还是无意，天灾还是人祸，保安还是保险，而是更为广义的安全状态 (SecSafe）。

* 世界环境与发展委员会出版的《我们共同的未来》报告中，将可持续发展定义为：“既能满足当代人的需要，又不对后代人满足其需要的能力构成危害的发展。”

——数世咨询，2023 年 11 月



以安全能力、数字资产和数字活动为三元素，以数据安全为核心目标，即三元一核的“数字安全三元论”。

“数字安全三元论”由“网络安全三元论”（数世咨询于 2020 年提出）更新迭代而来，旨在匹配数字中国建设的进程，保障数字基础设施稳定、可持续运行，保障数据有效流动、激发数据要素价值。

报告编委

主笔分析师：**闫志坤**　数世咨询合伙人 | 市场分析师
首席分析师：**李少鹏**　报告审核
分 析 团 队：**数世智库**　数字安全产业研究院

版权声明

本报告版权属于北京数字世界咨询有限公司。
任何转载、摘编或利用其他方式使用本报告文字或者观点，应注明来源。
违反上述声明者，数世咨询将保留依法追究其相关责任的权利。

目 录

前言 **1**

关键发现 **2**

1 API 安全概念 **3**

1.1 API 安全的关键能力 3

1.2 其他安全能力 4

2 市场指南 **5**

2.1 能力企业 5

2.2 市场概况 6

2.3 需求分析 9

3 未来发展趋势 **10**

4 API 安全代表厂商优秀案例 **12**

4.1 某大型银行 API 安全管控项目案例 12

本案例由**瑞数信息**提供

4.1.1 项目背景 12

4.1.2 项目目标 12

4.1.3 项目方案 13

目 录

4.1.4 项目成效 14

4.1.5 项目创新点 15

4.2 某医院 API 安全防护项目案例 17

本案例由青笠科技提供

4.2.1 项目背景 17

4.2.2 防护目标 17

4.2.3 防护方案 18

4.2.4 项目成果 18

4.3 某金融机构一体化 API 安全监测与防护 20

本案例由安胜华信提供

4.3.1 项目背景 20

4.3.2 防护目标 20

4.3.3 防护方案 21

4.3.5 项目创新点 23

前言

随着企业日益依赖API来提供对服务和数据的访问，他们对 API 安全保护的重视程度也与日俱增，API（应用程序编程接口）是现代软件开发的重要组成部分。它们是不同系统之间彼此通信以及共享数据和功能的“桥梁”。它为企业实现高效的数据共享、便捷的功能集成以及微服务架构改造等提供了技术支持，成为推动企业数字化转型的关键基础设施。

对 API 的日益依赖也使其成为网络犯罪分子最有吸引力的目标，通过攻击API来破坏信息系统和窃取数据，将成为数字时代黑产活动最集中的方向之一。然而，传统的API网关或WAF的防护已无法满足企业的API安全需求，数字时代需要专注于API的安全解决方案。

为了客观真实地反映API安全领域的市场及技术情况，数世咨询通过资料收集、问卷调研、企业访谈、市场数据分析等方法撰写《API安全市场指南报告》。本报告从应用创新力与市场执行力两大维度展现API安全厂商市场能力，同时，报告还对API安全概念、能力企业、市场概况、需求分析、未来发展趋势等角度进行了梳理与描述，供业内人士参考。

主笔分析师：**闫志坤** 数世咨询合伙人 | 市场分析师

勘误与合作联系：yanzhikun@dwcon.cn

关键发现

- 随着轻量级大数据技术的普及，促进了更多 API 安全产品涌现，新增了一批专注 API 安全的创新型企业；

- API 安全面临的最大一项挑战是全量 API 资产的发现与识别，而如何做好自动阻断功能，已成为业界共同关注的焦点；

- 目前 API 安全最大的应用场景是数据安全，除此之外，组织采购点需要主要集中在 API 资产发现与管理、风险监测、合规、访问控制、权限管理等方面；

- 目前API安全行业需求主要集中在政府部委、运营商、金融、互联网企业、电力；

- 在 HW、重保、攻防演练等场景中，API 已经成为重要的攻击目标，进而驱动了组织对 API 安全的需求；

- 2023 年国内 API 安全市场规模约为 6.5 亿元，预计 2024 年将达到 10 亿元。

1 API 安全概念

本指南中的 API 安全是指，以 API 生命周期为链条，在协议覆盖、资产梳理以及攻击检测的基础上，通过大数据分析、机器学习等技术，精准描绘出业务逻辑和数据流向，进而整合各种安全资源，以达到威胁预防、攻击阻断以及敏感数据泄漏防护等目的。

1.1 API 安全的关键能力

API 资产发现与管理

通过流量分析、读取 API 文档和配置、代码分析等多种技术手段，对多种 API 格式进行全面 API 资产识别发现（包括影子 API 和僵尸 API）、归拢聚合并实时更新，是做好 API 安全防护的先决条件，也是 API 安全面临的最大挑战之一。API 资产发现与管理贯穿整个 API 生命周期，其中主要工作包括业务 API 识别、分类打标、账号管理、容器 API 识别、资产拓扑等。

攻击防护

API 安全产品要能够阻止针对 API 协议的攻击，除了 plain HTTP、REST 等可复用传统安全能力的协议之外，仍有诸多协议标准，如 GRPC、Dubbo、GraphQL 等；还要能够阻断 WEB 攻击，尤其是针对 OWASP API Security Top 10 中定义的网络攻击。API 安全产品应该能够检测到针对身份认证、授权攻击，以及其他类型的授权攻击。它还应该能够检测到过度的数据暴露、缺乏资源或速率限制、安全错误配置、注入缺陷和批量分配缺陷等。此外，风险实时处置能力，如自动阻断或与现有安全处置系统联动形成闭环的能 力，已成为业界共同关注的焦点。

数据安全和隐私管理

数据管理也是API安全关键能力之一，需要具备敏感数据检测、数据地图、数据流转、数据出境、数据溯源等能力；同时要对敏感数据分级分类，满足《数据安全法》和《个人信息保护法》等合规要求，须根据不同业务场景对敏感数据进行分类和分级；数据隐私方面，通过加密技术、访问控制策略等手段，保护API传输的数据不被未经授权的用户访问或篡改和防范数据泄露。

智能分析

运行时防护：安全管控平台需要对API运行时的流量进行监测和防护，要实现这样的能力就需要了解API的访问、使用和行为，了解API安全环境的所有复杂性，解析日志、获取目录数据、审查配置、安全测试和评估设备配置等过程，利用综合数据解析API业务逻辑和行为，将其统一进行风险研判后，评估对API安全态势的影响，最后作出反馈动作。当然，AI/ML是需要时间去学习和改进的，对于行为分析来说，越早部署，安全效能的发挥就能越早体现。

攻击预防：在AI\ML的协助下高频的收集和持续分析API流量，并与每个源IP地址、每个用户和每个会话的攻击行为联系起来。因为攻击者在早期都会被动地、隐蔽地进行目标探测。还通常对客户端应用程序代码进行逆向工程以了解后端API的功能以及如何与之通信，这种被动分析技术可以逃避大多数检测，因为它们通常是作为合法流量出现的。而API安全产品应该能够检测到这样流量的细微变化，达到早期攻击预防的目的。

1.2 其他安全能力

- 应用威胁感知能力
- 运维降噪能力
- 情报输入输出能力
- 低代码/无代码防护拓展能力

2　市场指南

入选本报告的 API 安全厂商（按公司简称首字母排序）：安胜华信、安络科技、梆梆安全、保旺达、边界无限、从云科技、大拙信息、观安信息、联软科技、绿盟科技、美创科技、奇安信、青笠科技、全知科技、瑞数信息、上海喜数、深信达、数安行、腾讯安全、威胁猎人、芯盾时代、星阑科技、亿格云，共 23 家。

2.1　能力企业

根据厂商在 API 安全营收占比、业务专注度等多维度因素，将其划分为专业赛道厂商、综合业务厂商两大类，横坐标是市场执行力、纵坐标是应用创新力为依据，通过能力点阵图的方式展现如下：

图 1　专业赛道厂商

专业赛道厂商是指专注于 API 安全领域，核心业务围绕 API 安全产品、占据公司主要营收， 在 API 安全市场具有一定影响力、同行 / 客户推荐度较高的企业。

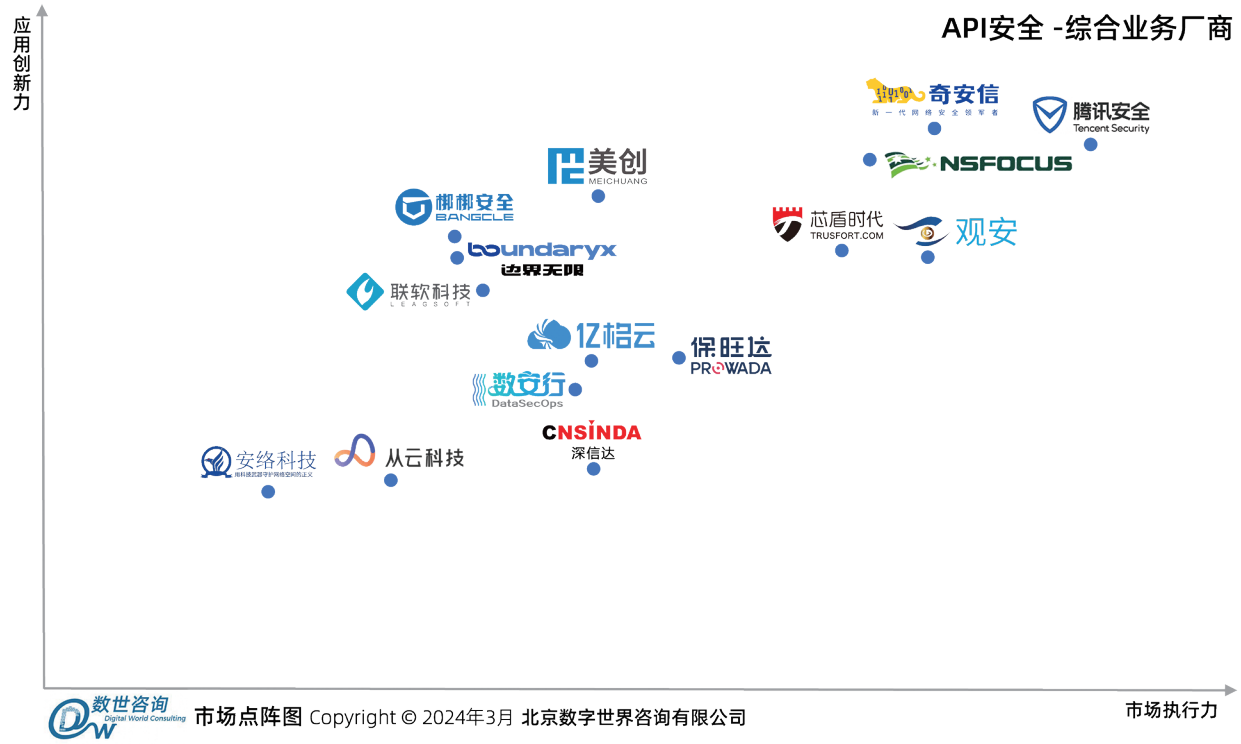


图 2 综合业务厂商

综合业务厂商是指业务范围广泛，不局限于 API 安全产品，通常将 API 安全产品与其他安全产品集成形成更全面的解决方案，满足客户多样化的安全需求。

API 安全点阵图横坐标“市场执行力”包括市场营收、品牌影响力、行业广度、行业深度等维度，纵坐标“应用创新力“包括产品工程化、业务场景化、理论与基础研究、技术融合度、业务纯净度等维度。

2.2 市场概况

目前 API 安全在国内市场处于“新兴市场”。在数世咨询《中国数字安全能力图谱 2024》属于“应用场景安全”方向中“互联网业务安全”的二级分类。

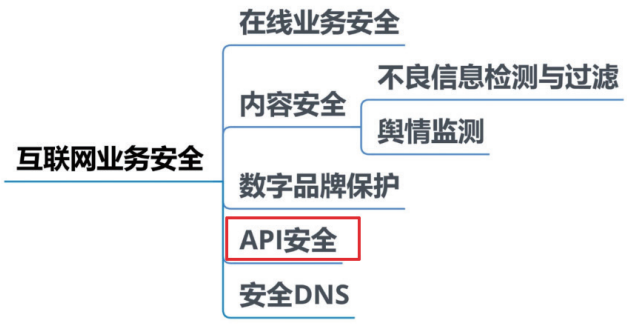


图 3　在《中国数字安全能力图谱 2024》位置

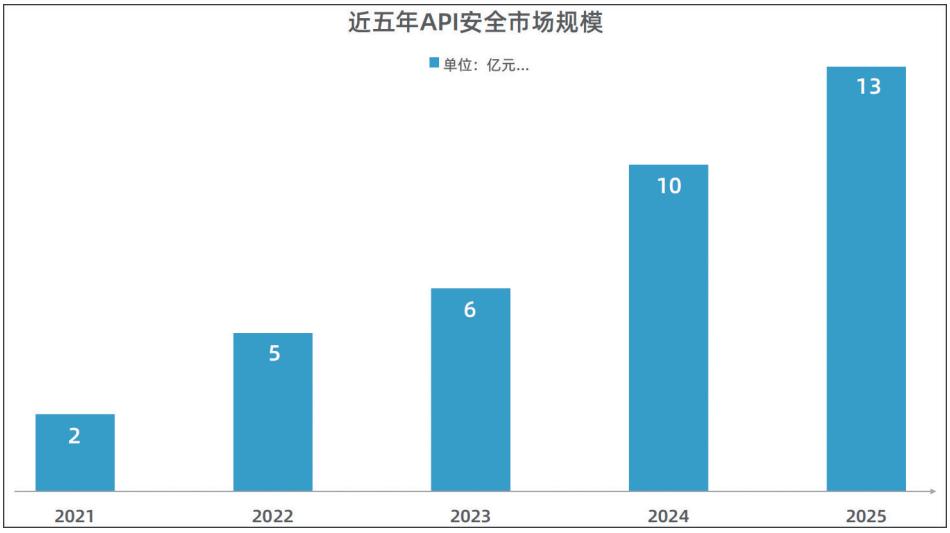


图 4　近五年 API 安全市场规模

据本次调研统计，2023 年 API 安全市场规模约在 6.5 亿元，根据参与调研的各安全厂商对本年 API 安全产品收入情况预估，预计 2024 年 API 市场规模预计达到 10 亿元左右，API 安全市场仍处于发展初期，未来增长潜力巨大。

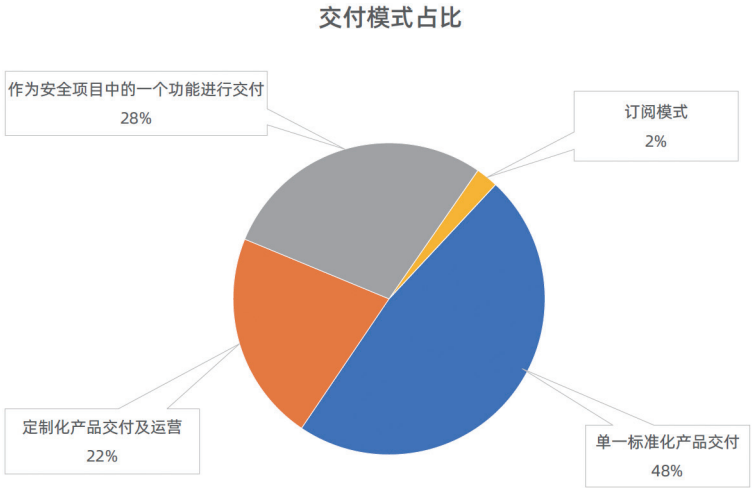


图 5　API 安全产品交付模式占比

其中产品作为单一标准化产品交付方式占 48%，定制化产品交付及运营占 22%，作为安全项目中的一个功能进行交付占 28%，订阅模式占 2%。

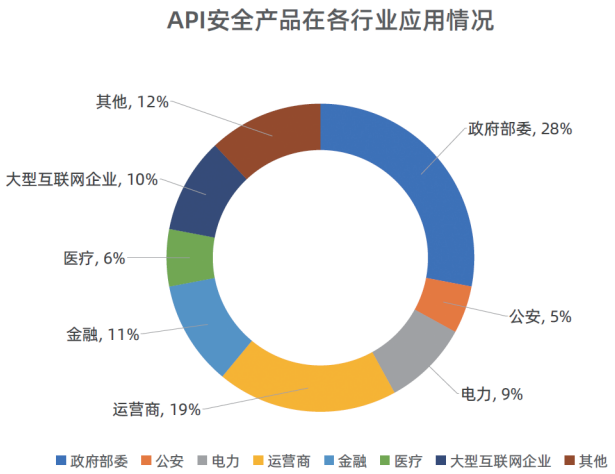


图 6　API 安全产品在各行业应用情况

根据调研结果，国内各行业组织对 API 安全的投入情况如下所示，前五名行业分别为政府部委（28%）、运营商（19%）、金融（11%）、互联网企业（10%）、电力（9%）。这些数据表明政府和涉及重要基础设施的行业对 API 安全需求和投入更为显著，特别是在 HW、重保、攻防演练等场景中，API 已经成为重要的攻击目标，因此，API 安全在保障数据和服务的安全方面具有至关重要的作用。

此外，互联网企业由于自身业务特殊性、复杂性，部分头部企业采用了自主研发 API 安全产品，来满足自身使用需求。

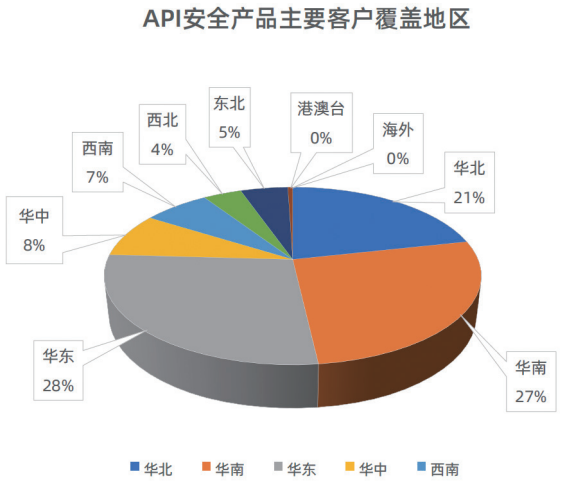


图 7　API 安全产品主要客户覆盖地区

此外，API 安全产品主要客户的覆盖区域也存在鲜明的特征，其中华南地区（27%），华东地区（28%），华北地区（21%）为主要的客户所在地区。这些地区在 API 安全产品客户中占据显著份额，反映出对 API 安全的明显需求。这种需求增长可能部分归因于这些地区拥有大量科技企业、互联网公司和其他高度依赖 API 的组织。

高占比的地区表明 API 安全提供商需要特别关注这些地区，提供个性化的市场推广和客户支持，以满足这些地区客户的需求。同时，也需要不断探寻其他地区的潜在机会，以扩展市场份额。

2.3 需求分析

根据本次调研，数世咨询分析得出，目前国内组织采购 API 安全相关解决方案的需求主要围绕以下几个方面：

API 资产发现与管理：全面梳理 API 资产，实现全生命周期管理，包括 API 发现、分类分级、变更管理等，难点在于影子 API 和僵尸 API 的发现和管理。

API 风险监测：识别 API 漏洞、数据安全风险和异常行为，并及时采取措施进行修复和防护。

API 访问控制：实施细粒度的访问控制和权限管理，确保只有授权用户和应用程序才能访问 API 资源。

数据安全：保护 API 传输和存储的敏感数据，包括数据加密、脱敏和防泄漏。

安全合规：满足相关数据安全法规和行业标准的要求，提供合规性检查和报告功能，帮助企业满足合规性要求。

3 未来发展趋势

1、数据合规和隐私保护愈加严格驱动 API 安全落地

随着政府和行业对 API 安全监管力度将不断加强，相应的法规和标准不断完善，企业必须重视 API 合规性，以规避监管风险。特别是数据分类分级、数据安全出境等方面，企业需要建立健全的 API 安全管理体系以满足合规需求。

2、API 安全技术向着智能化发展

未来，API 安全产品会具备访问风险实时检测能力 / 处置能力 / 溯源能力、低代码 / 无代码防护拓展能力等安全能力，我们将看到大数据分析、机器学习、行为分析等人工智能技术将在 API 安全领域进一步深化。

3、API 安全未来向着一体化生长型平台发展

API 安全将成为打通内部网络安全、数据安全和外部应用安全、业务安全的重要防护手段。未来，API 安全平台将在同一个数据平台上集成 API 安全治理、应用环境威胁感知、敏感信息流动监测、访问实体行为监控、业务逻辑安全等安全功能，向着一体化生长型平台发展。

4、API 安全平台与 DevSecOps 流程对接，强化 API 全生命周期安全

安全左移（软件物料清单、开发安全）是支撑 API 安全重要环节之一，API 安全平台将与 DevSecOps 流程对接，保护 API 生命周期中都得到安全保障。

5、新增基于业务逻辑的反欺诈功能

通过深度理解和分析业务流程中的逻辑关系，识别和阻止潜在的欺诈行为，并根据企业的业务特点和风险模式，定制化反欺诈规则和策略，提高识别准确性和防护效果。

4 API 安全代表厂商优秀案例

4.1 某大型银行 API 安全管控项目案例

本案例由瑞数信息提供

4.1.1 项目背景

近年来，某大型银行一直在积极寻求业务上的革新，借助互联网环境，通过 API 和 APP 等接入方式，为客户提供便利的服务；与此同时，该银行还经常搞一些促销活动。

然而，大量黑产通过工具抢促销，导致促销活动中有 2/3 的红包被黑产薅走，甚至出现了活动页面无法打开的窘境。因此该银行迫切需要采用创新的安全防护技术应对当前的业务风险，确保业务安全合规。

4.1.2 项目目标

信息泄漏防护

梳理已知和未知的 API 接口，防止 API 接口滥用，对 API 传输中的敏感数据进行识别，并进行脱敏或者实时拦截，防止敏感数据泄露。

业务威胁防护

防止攻击者通过 API 接口，批量发起业务攻击，避免在促销活动时发起薅羊毛攻击，以及在业务交易时发起交易欺诈的攻击，导致业务损失；防止撞库、爆破和重放等攻击造成用户信息泄露和账户盗用等危害，避免给该银行的形象

带来负面影响。

网络安全合规

在攻防演练中通过攻击防护、用户行为管控和用户画像等功能对 API 发起的攻击进行防护以及攻击溯源；通过API 资产生命周期管理避免在监管机构（银监、网监等机构）安全检查时发现未知的 API 接口及其它安全问题，免遭通告批评或者罚款。

4.1.3 项目方案

针对该银行面临的安全威胁，瑞数信息致力于为其打造一个包含资产管理、攻击防护、敏感数据保护和访问行为管控等的API 全生命周期的安全管控平台，具体如下：

图 8　API 全生命周期安全管控平台

资产管理：API 资产生命周期管理

引入 API 资产管理，实现对 API 资产的统一管理。API 资产管理基于数据建模自动发现被保护站点的 API 资产，并在报表分析中展示检测到的 API 请求，帮助客户实现 API 资产的生命周期管理。

API 自动发现：自动生成 API 列表，对 API 接口的访问情况一目了然。

API 资产分组：基于关键字快速分组，并在分组后指定责任人，实现资产

管理闭环。

API 导入和导出：支持从 API 网关、CMDB 等导入 API 列表，同时可以将 API 清单导出。

API 资产上下线：对 API 资产分组，进行批量上下线，实现 API 资产管控。

攻击防护：实现 API 资产纵深防御

通过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，从而有效检测威胁攻击。智能威胁检测引擎会在用户与 API 应用程序交互的过程中收集数据，并利用统计模型来确定 HTTP 请求的异常。一旦确定异常情况，智能引擎就会使用机器学习获得的多种威胁模型来确定异常攻击。

敏感数据管控：防止 API 接口数据泄漏

通过敏感数据管控对该银行业务的 API 接口回传报文的手机号码、银行卡号和身份证号码等敏感信息进行识别、过滤和脱敏，防止数据泄漏。与此同时，敏感数据保护功能会记录客户端访问 API 接口的时间、源 IP、账户、域名、路径和内容等信息，方便运维人员进行聚合分析以及追踪溯源。

访问行为管控：实现 API 多维度业务威胁感知

通过 AI 技术对 API 接口的访问行为进行多维度 API 基线核查和威胁建模分析，发现各种业务威胁；同时借助访问行为管控模块拦截各种异常访问行为。

4.1.4 项目成效

目前，该银行已经将个人网银、企业网银、微信银行、手机银行和直销银行等 20 多个核心业务系统均纳入瑞数 API 安全管控平台的防护范围。平台上线两年多来，没有出现任何故障，很好地为该银行抵御了因 API 接口而发起的各种漏洞攻击、注入攻击、跨站攻击、撞库攻击、薅羊毛和交易欺诈等，获得

了该银行的高度认可。

满足安全合规要求

瑞数信息积极配合该银行参与国家级网络安全重保、攻防演练和安全迎检等工作。在每年的攻防演练期间，瑞数 API 安全管控平台均发现并拦截了 10 余种攻击行为，300 万余次攻击次数，让该银行在行业内获得了良好的成绩，树立了良好的公司形象。

避免造成经济损失

帮助该银行提前做好防护，以主动应对通过 API 接口发起的攻击威胁，如：零日漏洞攻击、批量开户、撞库、信息泄露、薅羊毛和交易欺诈等攻击，避免遭受攻击以造成经济损失。

增加市场营销收益

帮助该银行拦截黑客利用大量虚假身份或盗用身份、模拟正常业务逻辑向该银行发起业务攻击，保证每次市场营销活动顺利进行，让用户可以真正地享受市场的促销优惠，从而达到“拉新促活”的目的。

降低安全运维成本

瑞数 API 安全管控平台无需修改应用代码、无需进行特征库及策略库的升级维护工作，不仅可以实现业务全天候运行，还可以节省安全评估、安全应急、安全运维、安全合规和攻防演练等方面的成本投入。

4.1.5 项目创新点

API 自动发现技术可以快速自动地发现业务潜在的未知 API 接口，并且针对发现的 API 接口给出综合评分，减少 API 接口防护的盲点。同时，通过清晰

的 API 列表辅助运维部门实时感知每个 API 接口的访问情况。

SDK 与各类 API 来源应用进行集成全渠道感知 API，增加 API 各种应用场景的防护，可以对来源环境和用户行为进行感知，将防护边界从服务器端延伸到客户端，通过客户端指纹追踪、真实性识别和行为分析等技术，快速过滤出具有攻击或欺诈意图的恶意来源终端；

全业务链安全威胁防护技术精准地构建 API 画像，运维部门可以快速预览各个业务的 API 情况，包括使用情况、异常情况和访问来源等，从而大幅提升对交易欺诈和黑客来源的识别及追踪能力，且能全程掌控业务威胁全貌，建立对抗网络空间威胁的全方位立体作战能力；

根据访问行为分析的结果或指定条件进行动态响应防护，如：阻断、延时响应和返回特定页面等，提升攻击者通过手工逆向分析或自动化工具探测等攻击手段对该银行业务发起攻击的难度。

金融行业经历了从网点模式到 APP 模式、再到如今的 API 模式的演进历程，API 的应用模式与业务场景和生态链接日益紧密，但是在 API 的应用过程中也引入了很多新的风险。该项目的成功经验，为金融行业成功探索出了一条保护 API 接口的新方法，该银行所获得的防护效果和项目收益，对广大金融企业具有很好的借鉴意义。未来，瑞数信息也将继续助力该银行和其他金融机构构建开放、合作和共赢的动态安全金融服务生态链。

实际上除金融行业外，截至目前，瑞数 API 安全管控平台也已在国内运营商、政府和企业等多家客户中广泛应用，通过采用全渠道感知 API、用户画像和动态响应防护等技术，帮助各行业企业主动应对通过 API 接口而发起的新兴威胁，全面保护在线交易、网站和数据的安全！

4.2 某医院 API 安全防护项目案例

本案例由青笠科技提供

4.2.1 项目背景

随着 5G、云计算、物联网等新兴技术与传统医疗系统的不断融合，医疗信息化程度不断提高，医疗数据呈爆发式增长，其蕴含的价值也随之提升。然而，这也带来了更多的数据安全风险。与此同时，国家、行业层面日趋完善的数据安全监管，使得医院数据安全建设面临更大挑战。

某医院近年持续推进智慧医院建设，为了给患者提供更便捷的就医服务，通过 web 网站、微信公众号、第三方支付等方式进行信息发布、预约挂号、报告查询等服务，内网业务应用对外开放大量 API 用于数据共享交换；API 接口的使用在医院跨网、跨机构间的业务协同和数据共享中发挥着高效的支撑作用，帮助医院实现诊疗、服务、管理、运营的正常运转。但往往也成为了外部攻击者攻击医院内部网络的通道，对医院系统和敏感数据造成极大安全威胁。

4.2.2 防护目标

API 接口全面梳理

全量梳理API接口、识别僵尸API接口、涉敏API接口，完善API资产清单;

敏感数据流动分析

监测涉敏接口敏感数据流动去向，识别合理身份下的违规使用、滥用数据行为;

安全风险审计溯源

通过异常行为检测和分析技术对 API 接口潜在的脆弱性风险（涵盖 OWASP

TOP10)、用户异常、行为异常等风险进行识别，并提供溯源处置方案；

参照现行法律法规和行业标准，确保 API 开放与数据共享过程中所有环节符合《网络安全法》、《个人信息保护法》等相关法规要求。

4.2.3 防护方案

通过在医院内网核心交换机旁路部署 1 台青笠 API 数据安全监测设备，对医院应用系统全量访问行为进行监测、分析，构建贯穿全安全运营周期「事前梳理－事中监测－事后溯源」的安全运营逻辑链；实现医院 API 资产可见、数据流动可视、安全风险可知可溯源。

事前梳理：基于流量协议解析技术自动梳理庞杂的 API 接口，并进行分类、打标，完善 API 资产台账；

事中监测：内置策略结合自定义专家策略实现对 API 脆弱性、用户异常、业务访问异常等安全风险进行识别。

事后溯源：全量访问行为审计留存，促进风险事件快速溯源定责。

4.2.4 项目成果

数据资产可见

通过全流量监测解析、智能化梳理实现 API 资产的梳理，帮助某医院清晰的感知资产情况、敏感接口分布情况，为院方安全决策提供基础，提升院方针对应用访问行为监测、分析、溯源于一体的业务安全监测能力。

数据流动可视

通过多维度数据透出统计分析，细粒度监测数据流动趋势，帮助院方对内

部业务数据流动、对外数据流动进行监测，识别合理身份下的数据非法使用、滥用行为，规避数据泄露风险。

安全风险可知

基于异常行为能力检测与分析能力，对接口脆弱性、用户异常、业务访问异常等行为进行检测，有效识别风险，并提供溯源、定位、处置能力，促进院方对风险事件的快速闭环管理。

安全事件可溯源

以全量访问日志记录为基础，集合多个维度的统计分析能力，帮助院方快速定位风险来源，分析风险事件主体，提供数据支撑，以及原始数据证据信息，满足合规需求。

4.3 某金融机构一体化 API 安全监测与防护

本案例由安胜华信提供

4.3.1 项目背景

随着互联网的高速发展，在数字经济快速发展的同时，API 已成为面向内外部业务输出、数据输出的重要载体，成为拉通业务 + 数据 + 应用的物质基础。API 置身其中，必须坚决维护网络安全，以国家安全观为指导，有效应对各种 API 安全威胁和挑战，维护网络秩序，共建健康、安全的 API 经济生态。

近年来，各大金融机构开始重视 API 安全风险，存量的安全运营架构中 API 安全监测能力不足，无法及时发现业务逻辑漏洞风险，还出现过未授权访问批量获取敏感信息问题。金融机构把控安全运营的主流建设方向中，希望做到 API 安全细颗粒度监测，但是一天动辄成千上万的风险告警量，也无法进行有效处理，因此，建立一套具备 API 安全检测能力的可持续运营体系迫在眉睫。

4.3.2 防护目标

通过接入全业务流量，识别业务数据，建立业务风险规则和数据安全规则，形成 API 资产发现、涉敏数据防泄露、规则模型及风险识别处置等多个方面的效果，完成对 API 攻击行为和 API 数据泄露行为的风险识别，阻断攻击 / 异常行为，降低安全事件的发生。即，专注于：数据与业务强关联场景下数据使用和流动过程中参数级的感知、检测、监测、分析与处置。

基于数据流量，动态提取 API 请求及响应数据，构建 API 数据资产。

事前：对自动化、越权、绕过等 API 攻击行为分析，建立以 API 数据资产为核心的防护模型；

事中：实时统计分析 IP、数据、访问行为等内容，匹配规则模型，对异

常行为告警并阻断；

事后：对留存的 API 访问记录审计分析，进一步优化检测模型，提升攻击 / 异常检测准确性。

4.3.3 防护方案

本次申报案例的方案内容主要集中在 API 风险全面检测、告警实时处置、可持续运营三个方面。

1、以 API 为技术角度，被动主动相结合，全面检测攻击行为

通过对 API 业务数据中的请求和响应进行识别，提取访问源地址信息，分析攻击者以自动化破坏性手段对业务系统发起的攻击行为，以及通过绕过、越权、参数遍历等行为发起的获取数据的非破坏性攻击性行为。针对短期内无流量的 API，采用主动检测形式产生流量，构造异常访问进行风险检测。通过主动被动相结合的方式对以 API 访问的所有攻击行为进行全面分析。

图 9　API 安全测试自动化示意图

2、插件部署，实现实时阻断，又不增加链路节点

基于业务字段级别的全量数据留存，针对业务上下文关联分析以及多维度的数据下钻、数据检索等各种个性化分析，短时间内溯源到安全事件的关键信息，然后进行阻断处置或者联动处置。

网关插件以脚本的形式部署在业务系统网关 Nginx 上，访问请求信息经过网关时，脚本对访问请求信息进行拦截并解析，先发送给平台完成攻击行为分析，再将结果返回至插件，**插件根据预设的交互条件确定通过还是拦截**。为避免影响业务链路的访问时效性，可在插件中**设置超时时间**，当拦截的 API 请求在超时时间内未接受到平台对风险的响应结果，**插件根据确定的目标地址继续向后发送请求**。

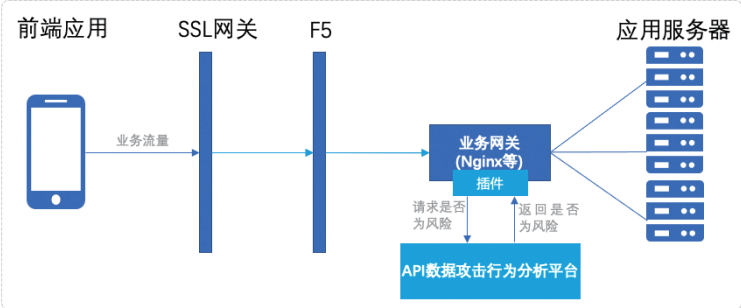


图 10　插件部署模式示意图

3、建立常态化运营机制，与三方系统联动，实现运营自动化

项目在实施过程中，**与自动化编排系统进行联动**，平台根据风险级别，将风险数据输出给自动化编排系统。对外部系统，实施请求拦截或者将 IP 从防火墙上直接阻断，将损失减少到最低；对内部系统，首先下发整改通知，要求人员确认漏洞和验证，平台根据修复的结果持续验证。以此**实现风险数据输出、风险联动处置及响应的完整机制和常态化的运营体系**，为后续的安全运营项目提供建设性的指导意见和经验积累。

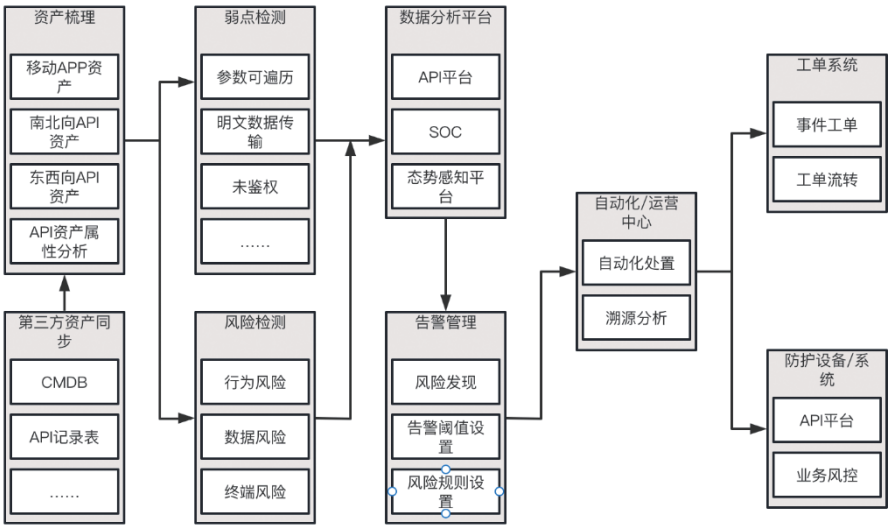


图 11　安全运营体系化示意图

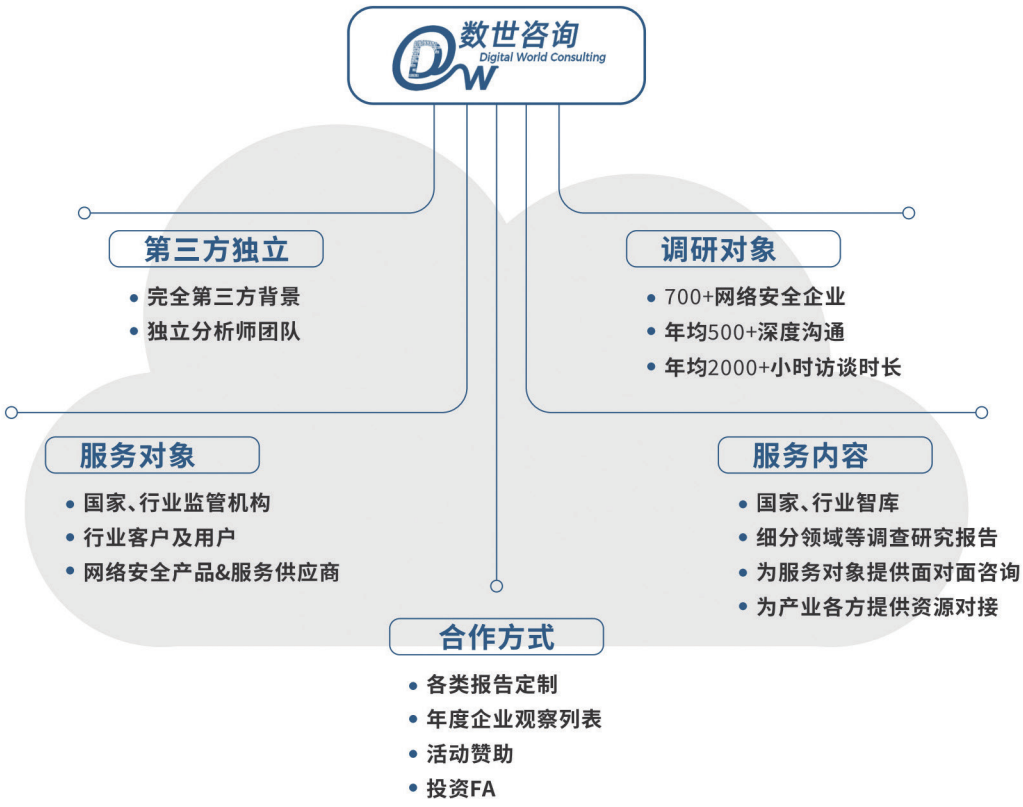
4.3.4　项目创新点

项目创新点主要体现在三方面：

一是覆盖范围方面，案例在数据攻击分析方面**涵盖 API 自身运行风险及基于 API 发起攻击的风险**，确保基于 API 的攻击风险和数据安全风险能够全面发现；

二是部署方面，**业务系统零改造，利用插件部署模式**，既不增加链路节点又可实现攻击拦截，实现会话阻断处置；

三是业务运营方面，**互联网风险与自动化编排处置系统联动，实现风险自动化处置，内网风险与数智化运维平台联动，根据业务系统反馈情况再行处置，处置率达标。**



北京数字世界咨询有限公司（以下简称数世咨询）是国内数字产业第三方调研咨询机构，主营业务为网络安全产业领域的调查研究、资源对接与行业咨询。在国内网络安全产业的调查研究领域，无论是专业性还是资源丰富性，均处于业界领先地位。

调查研究方面，撰写发布过《中国数字安全大事记》、《中国数字安全能力图谱》、《中国数字安全 100 强》、《中国数字安全产业统计》等业内影响力巨大的公开报告。同时，还为监管机构、国家部委、大型国企等单位提供各种定制化的内部调研报告。

资源对接方面，数世咨询目前已对接国内网络安全企业 700 余家，以及 150 余家有网络安全投资业务的资本方，建立了频繁且良好的沟通合作关系，包括共同举办会议活动，投融资对接，安全产品与企业推荐，企业资源整合等。

行业咨询方面，经常性的为监管部门、国家部委、安全企业、安全用户、一二级市场投资机构提供建议、企业培训及专家评审等咨询服务。

公司地址：北京市东城区鲜鱼口街 90-2 号网安小酒馆
官方网站：www.dwcon.cn
联系邮箱：dw@dwcon.cn

小酒馆

数世咨询
Digital World Consulting
数字安全领域独立第三方调研机构