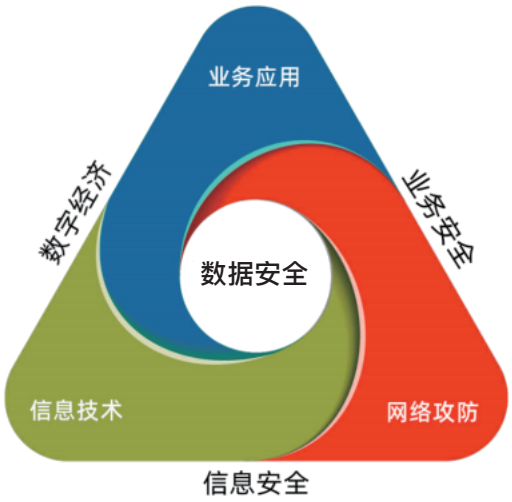
数世咨询
Digital World Consulting

实现持续链接的价值

数世咨询·API安全研究报告·2022

数世智库·安全不止于安全

2022年4月



信息技术 + 业务应用 ➔ 数字经济

信息技术 + 网络攻防 ➔ 信息安全

网络攻防 + 业务应用 ➔ 业务安全

2020年，数世咨询首创网络安全三元论，该理论由信息技术、网络攻防、业务应用、三个支点构成，其中：

- 信息技术是IT基础，没有保护对象，何谈保护；
- 网络安全的伴生、服务和对抗本质，决定了它将永远的场景化、碎片化和动态化；
- 业务应用既是信息技术与网络攻防的成本来源，也是这两者最终的价值所在。

数字世界的安全，即数字安全，内涵是以网络安全为基础手段、以数据安全为核心目的，并已经成为数字经济健康发展和社会活动稳定保障的重要支撑。

数字世界，安全共生！

版权声明

本报告版权属于北京数字世界咨询有限公司（以下简称数世咨询）。任何转载、摘编或利用其它方式使用本报告文字或者观点的，应注明来源。

违反上述声明者，将依法追究其相关责任。

报告编委

主笔分析师：金东东·首席战略分析师
分析团队：数世智库·数字安全战略研究院
报告审核：李少鹏·首席分析师

CONTENTS
目录

01 关键发现 /01

02 报告综述

关于API /02

发起背景 /03

研发目的 /04

03 API的价值分析

API广泛应用 /05

API-first /06

API经济 /07

04 API的安全风险分析

API已成网络攻击标靶 /10

API自身安全风险较大 /11

05 API的安全现状分析
复杂的API安全 /14
API安全的认知 /16
API安全的建议 /17

06 API的安全产品分析
国外最佳实践者 /19
国内最佳实践者 /21

07 API的安全参考框架
API安全参考框架 /26
框架说明 /27

08 报告结语 /30

关键发现

数世咨询 Digital World Consulting

1

API 逐渐形成了自身的技术和经济生态，在全球范围内被采纳，是公认的数字时代的价值链接基础。

2

API 已经成为网络应用流量最重要的出入口，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。

3

事实不断证明，传统的 API 网关或 WAF 的防护方式已无法再满足企业的 API 安全需求，数字时代需要专注于 API 的安全解决方案。

4

企业开展 API 安全建设，可以优先考虑以收敛、整合、智能、自动为核心的安全框架。

5

数字时代的 API 安全产品应该以 API 安全生命周期为线索，在解决协议覆盖、资产梳理以及攻击检测的基础上，通过深度学习的能力，精准描绘出业务逻辑和数据流向。通过对业务流量和数据的学习，整合安全资源，达到攻击预防、攻击阻断以及敏感数据泄漏防护的目的，最终实现 API 运行时防护的安全状态。

关于API

API（Application Programming Interface）较为通俗的解释是应用程序编程接口，由一组用于集成应用软件和服务的工具、定义和协议组合而成。

因API技术属于云原生代表性技术，并且API的应用与推广很大程度上依托于云计算的发展，数世咨询《数字安全能力图谱2021》将API 安全归纳于信息计算环境-云安全-云原生安全分类下。因目前API安全属于创新型市场，暂未形成较大份额，故没有单独分类。

图 1 数字安全能力图谱2021

数世咨询认为：

API作为一种软件接口，主要用来实现应用程序之间的链接。在数字时代，由于敏捷性需求和微服务架构的发展，API具有的传输数据和提供能力两大功能，将是创新技术框架和商业模式的一大重要支撑。

报告综述

发起背景

数字化的趋势是无法阻挡的，在数字时代，企业价值塑造需要由链条式转变为平台式。加之新冠疫情的影响，供应链的安全性和协作有效性、远程办公的紧迫性，也促使生态企业之间的整合逐渐加快了脚步。

为了应对数字时代的挑战，越来越多的企业已经在利用 API 的技术和经济模式来保证竞争力的延续。API 不仅仅适用于云计算、物联网和大数据分析等数字化场景，它还可以帮助企业发掘并维系客户、构筑全新的业务生态。

然而，随着 API 巨大价值的体现，API 攻击也呈现出指数级的增长趋势。据 Gartner 预测，“到 2022 年，API 将成为网络攻击者利用最频繁的载体，而通过攻击 API 可以非授权使用企业的应用数据”。Gartner 报告《Advance Your Platform-as-a-Service Security（25 August 2021）》已经明确地将 API 安全确立为保障 PaaS 安全的一个重要类别，该报告专注于指导企业如何提高 PaaS 的安全性，包括一个安全参考架构，显示了保护这些平台所需的内容，将 API 安全范畴独立于 WAF 和 API 网关，使其拥有了自己的功能分类。

虽然我们已经发现并且感知到，安全风险是阻碍企业数字化转型的最大障碍之一，但不得不重视的是，传统的安全技术被证明并不能有效地阻止 API 攻击，企业需要在现有防护基础之上的全新方法。

数世咨询认为：

数字时代的 API 安全产品应该以 API 安全生命周期为线索，在解决协议覆盖、资产梳理以及攻击检测的基础上，通过深度学习的能力，精准描绘出业务逻辑和数据流向。通过对业务流量和数据的学习，整合安全资源，达到攻击预防、攻击阻断以及敏感数据泄漏防护的目的，最终实现 API 运行时防护的安全状态。

报告综述

研发目的

本报告的核心，在于向用户展示一种适应于国内信息系统和商业市场环境，在现阶段可实际应用到生产环节和业务流程中的 API 安全参考框架。

通过调研和分析现阶段，我国 API 应用过程中的安全状况，结合国际方面对于 API 安全的研究，分析 API 在现代业务流程的塑造以及商业模式的变革中所发挥的巨大作用，分析 API 在数字时代可能面临的种种安全风险，结合已经被广泛应用的实践和理论，为用户展示 API 安全风险管控的理念。

数世咨询的核心理念为，数字时代、安全共生。希望通过本报告，能够切实解决用户在企业发展过程中出现的关于 API 安全的问题，实现数世咨询的第三方参考价值，帮助企业用户在数字浪潮之中屹立潮头。

链接应用程序和数据，已经被确定为API的核心功能和发展方向。链接客户和商业伙伴，已经充分展现出API的商业塑造能力。

不仅服务于个人，API也为许多企业的数字化转型提供了强大动力。对于软件研发来说，API就相当于编程语言中的库和类，研发人员越来越多地在API的基础上开发应用程序，实现对通用服务的重复使用和共享，以加速创新和推动企业变革。

API的广泛应用

现代 API 往往隐藏在网络应用之中，在日常生活中接触最为广泛和熟知的身份认证、电子支付、定位、语音转换等等基础数字服务，都是以 API 的形式来呈现的。

☑ 根据 Postman 的监测数据显示，API 已经在全球范围内被充分接受，并且呈现出持续增长的趋势。2021 年，通过 Postman 平台的 API 通信遍布全球 234 个不同国家，较同期增长 56%，API 已经几乎在全世界被开发和调用。

☑ 根据 Akamai 的监测数据显示，2021 年所有互联网流量的 83% 被 API 流量占据，API 访问量以 30% 的速度逐年增长，预计到 2024 年将达到 42 万亿次访问。

☑ 根据 GoogleCloud 的调查结果表明，其 API 平台 Apigee 的用户 API 流量在 2019 年至 2020 年期间同比增长 46%，已经达到 2.21 万亿次调用。这一增长反映了各行业数字化转型接受度的增长，越来越多的行业开展了数字化优先的业务战略。

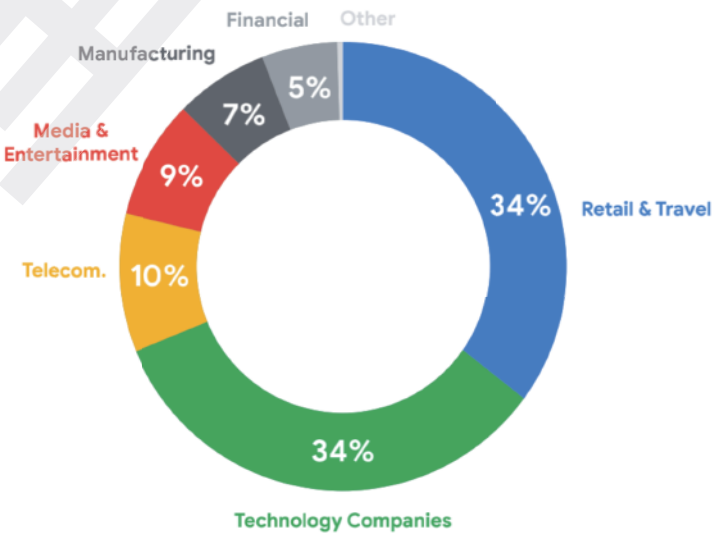


图 2 GoogleCloud 调研结果

从上图可以看到，GoogleCloud 的用户中有几个行业在使用 API 提高竞争力和效率方面特别突出。零售 & 旅游（34.5%）以及科技（34.3%）行业，它们占据了 API 流量的最大份额，而医疗保健（9%）和金融服务（5%）行业的同比增长却是最为突出的，增长率接近 200%。

数世咨询认为：

科技行业一直引领着技术潮流，API 的广泛使用反映了其经济模式和技术模式的成功，主要在供给侧产生积极影响。消费行业普及 API 则从市场层面反映了大众对于 API 的使用接受度，证明了 API 是完全符合现代用户体验的，主要从需求侧产生积极影响。医疗保健和金融服务因其业务承载的敏感性，通常会在一个新兴技术或模式相对成熟并且风险可控时进行业务匹配，而结合 API 技术发展和这两大行业的使用趋势可以看到，API 已经有能力成为数字时代应用和经济构建的基础。

API–first

数字时代的 API，可以看成是一种信息基础设施，因为它们将包含有关人和企业、事物的数据系统联系在一起，以便从这些数据中获取价值。企业的互联网业务、供应商沟通以及 SaaS 服务的连接，其核心都涉及 API 的使用。大部分企业通常在将其他软件解决方案与他们的 ERP 系统整合时开始使用 API。

1. 理念层面

API–first 在理念层面可以理解为通过实施以 API 思想为核心的整合战略来革新企业的业务和运营模式，通过使 API–first 与企业商业系统战略保持一致，支持商业模式转型。

企业商业系统战略的制定应根据商业目标和可衡量的成果来定义，而数字化转型就是其中最为重要的一部分。在数字时代，企业应该努力以新的方式做新的事情，为生态系统中的员工、客户和商业伙伴创造新的价值。

使用 API 参与到企业商业系统战略，可以帮助企业迅速实现数字化转型，开发新的商业模式，并使其能够有效抵御风险和抓住转瞬即逝的商机。数字化转型是大部分企业在市场环境混乱时期调整方向的一个机会，而 API 可以

通过促进这种转型来实现新的数字化产品和服务，以及新的商业模式。API在技术应用上是可行的，在资金投入上也是可行的，特别是针对数字化技术和商业平台服务。

2. 技术层面

API–first 在技术层面可以理解为一种软件研发的思想，指使用 API 作为访问应用程序和平台的首选方法，创建模块化、可重用、可扩展的软件架构。使用 API–first 思想是相对于其他信息系统集成方法的重大改进，因为 API 更容易实现、更强大、更不易出错，任何功能都可以作为独立的服务进行发布，在不影响其他功能的前提下，无缝链接到系统之中。

在云计算环境的普及和分布式服务的发展下，很少有业务流程是独立工作的，用户跨平台和设备的使用需求越发频繁，那么将不同的应用程序和功能快速、便捷的组合在一起并且高效发布，就成为了企业竞争力体现至关重要的能力。

3. 数字生态系统

Gartner 将数字生态系统定义为一组以实现互利为目的，相互依存的行为者（企业、人、物）共享标准化的数字平台，而 API–first 与数字生态系统是紧密相关的。

一个有效的 API 战略包括两个方面，应用整合与数字生态系统的整合。API 是企业应用战略的一个重要构件，包括可视化的整合、低代码应用开发和移动应用开发。企业高层必须意识到 API 是数字业务的核心，也是数字化进程的中心。创建一个 API 优先的战略，以满足数字业务的需求，确保数据和功能不被应用程序所限制。

API 也有助于开辟新的渠道，它们使初创企业能够在早期实现差异化并创造优势。API 帮助企业更有效地与客户、合作伙伴和员工搭建联系、增强体验，并在比企业预想的更大的范围内创造新的机会。

API经济

一项技术可以解决问题，而一种商业模式，却可以改变世界。就像云计算支撑了互联网模式一样，API 也正在形成自己的经济效应。

API的价值分析

数世咨询 Digital World Consulting

1. 模式价值

数世咨询认为：

对于做好充分迎接数字化时代的企业来说，API 完全可以作为创新的根基。API 经济模式主要有四种形式：

1) 链接能力、技术变现：作为拥有核心技术的平台型企业来说，可以通过 API 将自己的技术能力 SaaS 化输出，不断深化应用场景，扩大影响力。在国内市场，已经出现了一批成功应用，比如百度的自动驾驶、科大讯飞的语音转换、北斗卫星的地理定位服务等。

2) 链接数据、释放价值：作为数字时代的新生产要素，数据的价值是不可估量的。

大型互联网和科技企业都拥有自己的用户行为或业务大数据，通过 API 的形式将数据资源共享给企业内部团队，是企业创新的最佳方法；通过订阅的形式输送给用户，是企业盈利的一大手段。在国内市场，已经出现了一批成功应用，比如微步在线的威胁情报、字节跳动的用户行为、蚂蚁金服的消费趋势数据等。

依托于隐私计算和联邦计算的发展，政务数据可以通过脱敏和隐私屏蔽的方式，将数据资源开放给专业的企业进行业务创新，充分发挥出数据隐藏的巨大价值。在国内市场，已经开始了试点项目的论证与实验。而对于国家机构数据的商业化使用，国内早已出现了一批成功应用，比如气象信息、遥感信息数据等。

3) 链接生态，扩大战场：通过 API 进行有效的业务整合和协作。使用多个企业的 API 来创建自己的服务，通过业务场景进行服务的编排再出售，服务于不同的用户群体。增加企业上下游之间的粘性，通过 API 更好地获取资源并与自身业务集成，通过 API 快速和便捷地触达用户。

4) 链接流程，提质增效：企业内部管理环节的模块化，有助于随时根据战略要求进行适当的变更，减少不必要的时间浪费。企业内部业务流程的模块化，有助于信息共享和高效协同，提高技术能力的转化效率。

2. 生态价值

对于数字时代而言，API 经济是一套基于功能安全访问和数据交换的新商业模式和渠道。API 使万事万物更容易整合和连接，例如人、位置、系统、数据 、事物和算法。API 还能创造新的用户体验，分享数据和信息、验证人和事物、加速和保障交易、接入第三方算法，同时创造新的产品和服务。

在 API 经济中，企业必须认识到，API 生态的范畴是超越技术层面的，它是企业的商业模式、数字战略和生态系统建立的基础。

API 生态的最大价值是它可以推进企业发展成为行业、能力或监管的平台型组织，这类组织的三大特征包括：

1) 数字商业模式：使人、组织和业务组成的生态系统能够由表及里的创造价值。

2) 商业模式平台：通过利用现有的企业资产，如算法、技术、资源和分析，实现数字业务。

3) 商业生态系统：利用商业模式平台来创造新的解决方案。

API 拥有的这种能力将引起企业根本性的变革，影响业务和运营的许多层面，促进企业从新塑造适应于数字时代的商业模式。平台使价值创造成倍增加，因为它们使企业内外的商业生态系统能够在用户之间完成匹配，并促进商品、服务和经济与社会价值的创造和交换，从而使所有参与者能够从中获取相对应的利益。

我们已经清晰的认识到了 API 自身的经济价值，而且随着 API 链接的数据价值在不断增加，对于黑产和网络部队来说，API 就是头号目标。攻击者早已意识到，API 往往是企业应用安全链条中最薄弱的环节，特别是由于确保 API 安全的传统工具和方法不断被证明是不够的，还有许多安全意识的问题也会使企业、合作伙伴和客户处于风险之中。

API已成网络攻击标靶

☑ Facebook ViewAs 接口漏洞

2018 年 10 月 12 日，Facebook 公布了被大规模网络攻击事件的细节，此次事件预估造成了 3000 万用户的账号信息被泄漏。

Facebook 表示，黑客利用了 Facebook“ViewAs”功能接口中的三个漏洞。“View As”功能可以让用户看到他们的个人主页的展示样式，这给黑客提供了获取攻击的机会。这个问题自 2017 年 7 月以来一直存在，但直到今年 9 月 14 日，Facebook 才首次发现可疑活动增多，这也最终导致了 9 月 25 号大规模攻击事件的发生。

☑ 淘宝 mtop 接口非授权使用

2020 年 8 月，淘宝（中国）软件有限公司报警称，2020 年 7 月 6 日至 13 日之间，有黑产通过 mtop 订单评价接口绕过平台风控批量爬取加密数据，爬取字段量巨大。7 月 6 日至 13 日之间平均每天爬取数量 500 万，爬取内容包括用户评价内容、昵称等敏感字段。经淘宝网站排查，逯某有重大作案嫌疑。

经司法鉴定，逯某通过其开发的软件爬取淘宝客户数字 ID、淘宝昵称、手机号码等淘宝客户信息共计 11.8 亿条，逯某将其爬取信息中的淘宝客户手机号码通过微信文件的形式发送给黎某使用，共计 1971.26 万条。

☑ API 攻击泛滥成灾

据 Gartner 预测，“到 2022 年，API 将成为网络攻击者利用最频繁的载体，而通过攻击 API 可以非授权使用企业的应用数据”。

根据 Akamai 的攻击监测数据，其表示如今网上的大部分流量都是基于 API 的，Akamai 观察到的网络攻击，几乎肯定是针对拥有面向公众应用程

序和服务的组织。

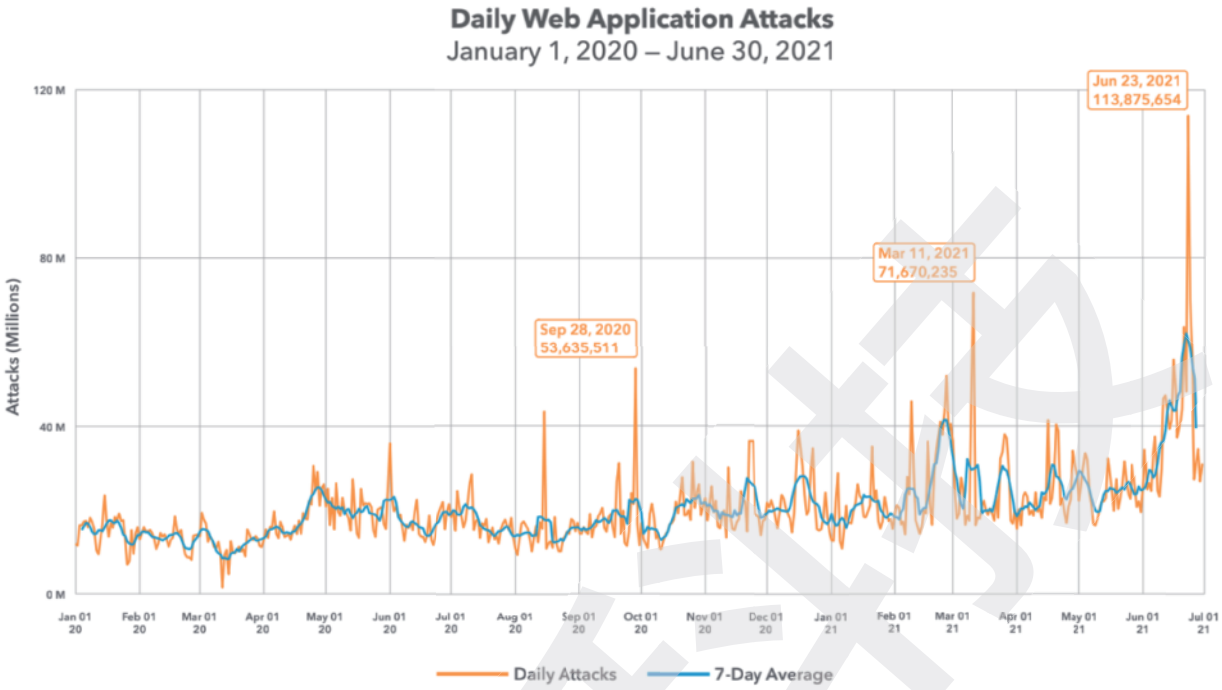


图 3 WEB 应用攻击监测

上图显示，在 2021 年 6 月单日观察到 1.138 亿次与 API 有关的攻击，是 2020 年 6 月观察到的攻击数量的三倍多。其中 SQLi 脱颖而出，成为过去 18 个月的头号攻击特征，记录了 62 亿次攻击尝试。排在第二位的是 LFI 有 33 亿次攻击，最后是 XSS，有超过 10 亿次的攻击。

API自身安全风险较大

事实证明，API 已经成为网络攻击的靶向目标。当 API 遭受到攻击时，可能引起诸多风险，如数据泄漏、数据丢失、账户滥用、服务中断、诈骗等。

1. 国际应用安全研究

OWASP 一直致力于研究和引领 WEB 应用程序安全，根据其最新发布的 Top 10 报告，可以直观的感受到 API 的安全风险。

表 1 OWASP Top 10 对比

OWASP Top 10 对比		
排名	**OWASP Top 10-2021**	**API Security Top 10-2019**
TOP1	Broken Access Control	Broken Object Level Authorization
TOP2	Cryptographic Failures	Broken User Authentication
TOP3	Injection	Excessive Data Exposure
TOP4	Insecure Design	Lack of Resources & Rate Limiting
TOP5	Security Misconfiguration	Broken Function Level Authorization
TOP6	Vulnerable and Outdated Components	Mass Assignment
TOP7	Identification and Authentication Failures	Security Misconfiguration
TOP8	Software and Data Integrity Failures	Injection
TOP9	Security Logging and Monitoring Failures	Improper Assets Management
TOP10	Server-Side Request Forgery	Insufficient Logging & Monitoring

OWASP API Security Top 10–2019 显示，排名前十位的安全风险依次为：失效的对象授权、失效的用户授权、过度的数据暴露、资源缺失和速率限制、失效的功能级授权、批量分配、安全配置错误、注入、资产管理不当、日志与监控不足。

从上表不难看出，API 安全风险与网络应用风险高度重合（相同颜色的标记代表同类风险）。这就意味着，API 除了自身的独特漏洞和相关风险外，API 也面临着基于网络的应用程序多年来一直在解决的同类问题。

2. 国内攻防实战经验

API 在我国商业市场上的应用已经在大型企业和创新型企业内普及，近年来也呈现出极大的增长率，而且开始出现在中型企业的业务逻辑中。但是，对于 API 安全风险的管控，却是所有企业都面临的一大难点。

在由公安部组织的，可控环境下的网络攻防实战演习中，通过利用 API 安全风险直接侵入、越权信息系统的方法效果显著。并且由于 API 的特殊性，使得攻击者拿下 API 后，可以直接接触到敏感数据和信息系统的重要操作权限。

通过与安全专业厂商的探讨，我们总结了以下国内真实业务环境中的 API 安全风险：

1）水平越权：利用失效的对象授权通过遍历参数批量拖取数据。

2）敏感数据暴露：脱敏失效，或一次性返回多余不必要的敏感数据。

3）代码漏洞：SQL 注入、命令执行，由业务开发者导致的风险。

4）API 基础设施漏洞：API 后端中间件、基础设施漏洞，如 log4j2、APISIX 漏洞。

5）错误配置：不安全、不完整或者错误的配置，如临时调试 API、未鉴权 API、存储权限公开、不必要的 http 方法、跨越资源共享等。

6）业务逻辑缺陷：无校验、无防重放、无风控策略、高并发导致条件竞争等。

数世咨询认为：

云原生、微服务、DevOps 实践带来的敏捷开发和 CI/CD 加速了对 API 的依赖。攻击者目标的集中，尤其是安全性不足的 API 就相当于没有防护的 VPN，导致 API 给企业带来了越来越大的安全风险。确保 API 的安全需要考虑许多不同领域，不仅仅是访问控制，重点还要包括网络、数据、业务逻辑和应用代码等。企业还需要管理并发展自身的 API 安全策略，从高层维度通过技术、管理和意识来保护自身的业务、用户和数据。所以，API 安全防护是一个体系化的问题。

复杂的API安全

API 从根源上来讲即一段程序代码，随着技术的发展和架构的变迁，API 相关标准和规范也在不断演进。现今，JSON Schema 是迄今为止使用最多的规范，接下来是 Swagger 2.0 和 OpenAPI 3.0。协议方面，从主要是内部的 XML 和 SOAP API 演变为更公开的 REST、GraphQL 和 gRPC。

国内范围中，主要对 API 的接入和管理规定了相关基础的标准。如 GB/T 35273-2020《信息安全技术 个人信息安全规范》、GB/T 36478.4-2019《物联网 信息交换和共享 第 4 部分：数据接口》等。还有一些行业，如通信、金融等，编制了针对行业的 API 使用标准，这里不做赘述。

除了标准和规范之外，API 安全的复杂体现在更多方面：

1) 作为微服务架构和云原生设计模式的结果，API 的数量和分布呈指数级增长，为安全管理带来了挑战；

2) 加速创建 API 以促进业务，并与客户以及生态伙伴交换数据，加之敏感信息保护越来越受到关注，使 API 安全风险陡然加大；

3) 许多企业拥有自己特殊的 API 架构和业务逻辑，通用化的安全方式不能很好契合；

4) 互联网产品形态的不同，需要不同种类前后端代码的支持，作为链接的 API，安全控制很难把控；

5) 网络攻击逐渐进化，除利用漏洞外，更多以滥用业务逻辑和访问控制规避的方法来进行。

我们可以这样设想，把 API 比做地下水资源。对于一个小型自来水厂来说，

只拥有一根地下水管，服务范围为一个居民社区。这样一个简单的业务，维护其安全性只需要几个人轮流对生产设施进行检查和维护，把守住唯一的出入口进行控制来防止投毒、破坏等事故的发生。

但是对于一个大型自来水厂，他拥有许多地下水管，服务着一个区域甚至一个城市的居民。它拥有各种资产、各种规模的建筑和重要设备，不同级别的访客会访问并进入各种建筑，其中各种建筑还包含不同的楼层，分布着不同级别的信息和访问限制。

对于这个水厂来说，保护其安全性就是一项极大的挑战，需要不同层次的安全方法来提供保护能力。为了注意可疑的活动，防止有人进入他们不应该进入的地方，企业不能简单地依靠几个人在入口检查，而是需要一个更复杂的解决方案，比如添加监控来观察资产、在水厂周围巡逻来寻找可疑的活动、在每扇门和窗户上安装传感器以及其他复杂的解决方案。对于这个水厂，我们将周边的安全与整个水厂的安全层层结合起来，以保护重要资产的多样安全性。

传统的 WEB 应用程序类似于上面提到的小型水厂，企业可以依靠传统的安全解决方案（如 WAF、API 网关等）来保护它们。这些解决方案以边界为基础，寻找已知的威胁来阻止风险的发生，同时让所有看起来正常的流量通过。而新一代的 WEB 应用程序是基于 API 的，除了更复杂之外，也更独特，如大型水厂的业务范畴。除了安全链条中的其他传统解决方案外，这些都需要一个现代和多功能的解决方案。

企业不能再用一个单一的传统解决方案来确保 API 的安全。传统的解决方案基于签名或已知模式工作，只能保护企业免受常见的、已知的攻击，如 SQL 注入（SQLi）、跨站脚本（XSS）和跨站请求伪造（CSRF），传统的解决方案不能有效检测 API 独特逻辑中的漏洞。除此之外，这些曾经流行的安全风险，由于现代应用架构和开发的最佳实践，其危害程度已经变得不那么大了，比如跨站请求伪造（CSRF）和一些跨站脚本（XSS）攻击在许多现代网络应用中已经不能被简单利用，因为它们几乎不再使用基于 cookie 的认证。

攻击者并没有放弃，他们在不断进化、与时俱进。企业的 API 是复杂而独特的，攻击者利用这一点，寻找独特逻辑中的漏洞，这些都是无法通过签

名来识别的。企业的 API 保护解决方案必须能够理解独特的 API 逻辑，以识别潜在的漏洞并阻止攻击。

API安全的认知

1. 逐渐失效的传统方式

数世咨询通过调研发现，在现阶段，我国企业大部分都依靠分析日志文件来识别 API 攻击者和事件，超过三分之二的调研用户正在使用 WAF 或 API 网关进行防护，但每个调研用户依旧都遭遇到许多 API 攻击。WAF 和 API 网关缺乏建立流量或逻辑关联活动的能力，导致经历过 API 攻击的企业依然在承受损失，这种安全防护方法被证明是不够有效的，是不能很好满足企业安全需求的。

对于企业来说，目前最关心的安全风险是僵尸 API 和未知 API。敏捷性带来的 API 频繁变化，使得旧版 API 在废弃时没有被完全消除，而大量的新部署和第三方 API 没有全部进行登记和测试，这些情况都是企业亟待解决的。

而当我们与调研用户谈论 API 安全时，很多安全事件往往可以追溯到 OWASP API Security Top 10。许多企业认为，只要处理好认证和授权就可以免受 API 攻击的侵扰，然而事实却是，绝大多数 API 攻击都是针对已经通过认证的 API，例如失效的对象级授权、失效的用户级授权和过度的数据暴露等情况。

并且这些 API 安全风险只是其中一部分威胁，攻击者通过许多其他方式发现和滥用 API。数字时代的企业还面临着来自自动化威胁的风险，包括扫描、撞库和破解等。最后，攻击者以新的逻辑将多个漏洞和滥用方式组合在一起，形成更加复杂的攻击链，能够逃避检测和保护，提高攻击者的成功机会。

2.API 安全的差异

近年来，网络应用程序的构建和交付方式发生了巨大的变化。现在，包括智能设备和物联网设备在内的客户端已经变得更快、更强大，而且浏览器能够执行越来越复杂的任务，许多曾经在服务器上完成的逻辑已经转移到了客户端，它可以运行复杂的任务并执行许多动作，最终在客户端上动态地呈现。

这种基于 API 的应用程序模式暴露了更大的攻击面，因为传统的应用程序暴露了少量的 HTML 页面，而基于 API 的应用程序暴露了大量的 API、API 端点和大量敏感数据。除此之外，数字应用环境有许多不同类型的 API，例如移动应用 API、微服务 API、第三方 API 和外部合作伙伴的 B2B API。

流量模式的变革使得客户端和服务器之间的流量在基于 API 的应用中看起来完全不同。在传统应用的情况下，客户端在请求中发送的数据较少、而服务器的响应包含大型和复杂的 HTML 页面。在基于 API 的应用程序中，客户端在请求中发送更多的参数，在响应中从服务器接收原始数据。请求和响应都更加标准化，有统一的格式、标准，这就让后端服务器已经变得更像一个数据源。

这种基于 API 的应用程序模式对安全和 API 保护同样产生了巨大影响。企业需要关注更多新的攻击载体，因为基于 API 的应用程序为新的攻击类型打开了大门，这些攻击通过 API 在非常细化的水平上学习应用程序的逻辑，直至了解每个单独的终端。然而这种模式也可以使用新的检测方法，因为基于 API 的应用程序的请求和响应通常是标准化的，拥有统一的格式，标准化的格式经过 AI/ML 的学习就能让监测流量和检测可疑活动变得更加方便。

API安全的建议

攻击者越来越频繁的使用自动化手段来攻击 API，防护手段也需要自动化。ML 和 AI 对于发现 API、查看 API 暴露的敏感数据以及检测和阻止攻击者都至关重要。越早的部署和使用人工智能，让其接触到生产环境和业务场景，就能越早的改善学习和调整结果。

安全意识也是必须正确面对的问题，API 安全通常被视为开发团队的责任，这种观点可能意味着企业会忽略部署针对性的保护措施，如运行时安全。在实践中，并不是所有的 API 安全问题都能在运行前的代码中得到测试和识别。

许多企业会选择外包服务，而第三方服务者很少会提供源代码，企业也缺少要求其证明安全性的方法。更关键的是，许多 API 的部署也使用基

础设施内的控制组件，如 IP 地址过滤、拒绝列表或速率限制机制。API 攻击通常都针对业务逻辑缺陷，这些缺陷不会在静态或动态分析安全测试工具中显示出来。

企业需要建立 API 安全生命周期的安全防控，特别是要确保在运行时的安全状态。在开发 API 时对其进行审查，在对接应用程序时自动进行生产前扫描，在时间允许的情况下进行彻底的人工测试，并部署运行时保护。

版权所有

数世咨询认为：

在商业市场，安全行业有两大核心价值。一是保障信息系统健康、持续地运行，一是促进业务发展、创造新的生命力。

数字时代选择了 API，安全行业就要肩负起保障和促进 API 发展的责任。从国际范围来看，对于 API 安全产品来说，已经诞生了一批具有应用场景和保障效力的最佳实践。

国外最佳实践者

☑ Apigee

Apigee 成立于 2004 年，于 2010 年进入 API 管理市场，2016 年因其 API 安全管理和分析平台的出色表现被 Google 以 6.25 亿美元收购。它提供的核心服务是帮助 Google 将人工智能的能力架构在其云平台上，同时也继续提供其他企业内部 API 安全管理服务。

Apigee 的旗舰产品是 Apigee Edge，是用于设计、管理和分析 API 的平台。它包括一套 API 服务，用于管理、保护和扩展具有额外后端功能的 API；一套分析服务，用于收集、分析和报告各种技术、运营和计费统计数据；一套开发者服务，用于围绕 API 建立一个社区。

Apigee 平台功能涵盖 API 生命周期每个阶段的安全与管理，内部实现复杂但对用户较为友好的策略管理，通过 Apigee Sense 扩展的运行监控和安全分析功能，与其他谷歌云网络攻击和 DDoS 保护服务的深度整合。

☑ Salt Security

Salt Security 是由以色列国防军校友于 2016 年成立的，在 6 轮融资中共筹集了 2.71 亿美元的资金。最新融资是在 2022 年 2 月 10 日的 D 轮，筹集了 1.4 亿美元的资金。目前为止，Salt Security 估值为 14 亿美元。投资机构 CapitalG 认为，Salt Security 是 API 安全市场的先驱，拥有真正有效和易用的企业级解决方案，基于 API 安全发展的趋势，对 Salt Security 产生了极大的认可。

Salt Security 拥有自行研发的统一 API 威胁保护平台，利用人工智能、大数据和行为分析的技术，保护 SaaS、网络、移动、微服务和物联网应用程序免受 API 威胁的影响，该平台不需要任何配置，可以在几分钟内部署。

与 WAF 等传统解决方案不同，Salt Security 采用无签名的自适应学习方法，不需要监督或配置就能识别和防止 API 攻击。它将识别活跃的 API 攻击，向 SIEM 解决方案发送警报，通过为安全分析师提供数据支持和为开发人员提供建议来帮助缓解安全风险，或与现有的安全设施集成以进行控制。

Salt Security 拥有诸多自主知识产权，以及在市场上多年成熟的 AI/ML 算法，从一开始就引领了 API 安全市场。并且制定了 API 保护的标准，通过其平台产品可以自动和持续地发现整个客户环境中的所有 API，利用云规模的大数据来确定和阻止攻击者，并在构建阶段识别 API 漏洞。

据 Salt Security 的创始人之一 Michael Nicosia 的发文显示，在过去的一年里，收入增长 500%，客户群增长 300%，员工人数增长 250%，签约的全球 500 强企业增长了 900%，其中包括武田制药、BP Launchpad 和 Markel 等可以公开报道的企业。

☑ Noname Security

Noname Security 成立于 2020 年，在 3 轮融资中共筹集了 2.2 亿美元的资金，最新融资是在 2021 年 12 月 5 日的 C 轮，筹集了 1.35 亿美元的资金。目前为止，Noname Security 估值为 10 亿美元，成为全球数字安全领域目前为止发展最快的公司之一。

Noname API 安全平台是一个带外解决方案，不需要代理或大面积网络修改，通过 API 态势管理、API 运行时安全和 API 安全 SDLC，提供涵盖整个 API 安全范围的解决方案，并提供比 API 网关、负载均衡器和 WAF 更深入的可见性和安全性。

Noname API 安全平台可发现各种类型的 API，以及未被 API 网关管理的问题 API，对所有 API 的进行梳理。使用自动化的人工智能和基于 ML 的检测来识别最广泛的 API 漏洞。实时防止攻击，积极进行 API 测试，修复错误配置，与现有安全措施相整合、联动。

Noname Securit 在成立第一年就获得了 2.2 亿美元的融资，这笔资金用于进一步加快全球市场推广工作，并继续投资于 API 安全创新。Noname Securit 从 2020 年的 4 名员工到现在的 200 名员工，并且全球范围内还在不断增加，只用了不到两年时间。

据 Noname Securit 创始人之一 Oz Golan 发文显示，公司的使命是通过帮助确保 API 的安全，使企业加快他们的数字化转型之旅。在过去的一年里，通过 Noname API 安全平台以不同的方式处理 API 安全问题，这使得他们赢得了世界上最大品牌的信任，成果是与全球 500 强中的 20% 建立了合作，帮助他们保护数字环境免受不断增长的 API 漏洞的影响。

国内最佳实践者

1.API 安全作为辅助

数世咨询认为：

在我国数字安全市场中，对于现阶段的 API 安全产品来说，API 安全防护能力通常被当作一个产品或解决方案的一部分，作为辅助功能来使用，导致这一现象主要有两方面的原因。

最主要的一方面是甲方需求不明显，市场价值不易显现。API 技术和模式尽管已经在大型平台企业内普及，但是传统制造业和中小型企业却明显没有跟上时代的步伐。据市场粗略统计，只有不到 11% 的企业明确了组织内部对 API 安全的管理和策略，至少 40% 的企业没有任何针对 API 安全的措施与计划，约 50% 的企业只是知道 API 需要安全防护但没有实际投入或只使用了传统的安全防护方式。

另外一个次要方面是安全公司缺乏引领性和创新性。国内安全市场长期以来主要以国家政策和监管市场为主，以销售额为导向，这使得安全产品和解决方案往往出现在强需求和严处罚的环节中，具有前瞻性和引领性的科技创新很难获得市场的验证和投资方的肯定。

当前我国 API 安全产品或解决方案大致有几种类型：

1) 侧重统一管控，全生命周期的 API 管理涉及 API 的规划、设计、实施、测试、发布、运营、调用、版本管理和下线等 API 各个生命周期阶段。API 管理工具使 API 生态系统和发布的 API 能够安全地运行，并收集分析结果用于监测和商业价值评估，这些功能通常被打包成工具集、策略管理和统计分析的组合。

数字时代，全球各地都在不断推进数字化转型的进程，数字化转型推动了 API 使用的增加，这反过来又增加了对 API 创建、管理、运营和安全的需求，并使全生命周期的 API 管理成为每个企业亟需具备的基本能力。由于需

要连接系统、设备和其他业务，各组织正面临着 API 数量的激增。在内部、外部、B2B、私人和公共数据共享中使用 API，推动了使用全生命周期 API 管理来治理 API 的需求。

云计算和云原生架构的普及正在增加 API 在软件架构中的使用，特别是在微服务、服务网格和无服务器的背景下。全生命周期的 API 管理为治理 API 提供了必要的框架和工具，使用这些工具进行业务活动，可以在有效开展工作的基础上同时保护企业免受 API 漏洞的影响。

2) 侧重数据安全，核心是 API 数据管理，主要实现敏感数据发现、脆弱性评估、脱敏、审计、安全态势展现等数据安全功能。API 数据的分级分类，安全策略、规则、场景的灵活配置，核心数据和敏感数据的发现与阻断等，都是企业面对的数据安全难题。

自动化的核心数据和敏感数据发现，监控用户访问记录并自动归纳分析，依据安全策略自动响应的 API 数据安全能力，将有效降低数据风险、提高安全效率、改善组织的合规性和数据保护状况，实现数据安全策略集中化管理，安全风险统一管控、集中运维的能力。

近年来，我国陆续发布了有关网络安全和数据安全的相关法律、标准、管理办法，明确了数据安全事件的责任与处罚标准。在数字时代，数据安全已经同网络安全处在一个认知维度，对于数据安全的防护，是企业必须极度关注的重点。

3) 侧重威胁防护，核心是对 API 的防御，使其免遭滥用、非授权访问和拒绝服务攻击，这个能力对外部和内部的 API 都是必需的。API 网关、WAF 以及专业的 API 安全工具通过 API 参数和有效载荷的内容检查、流量管理和异常检测的流量分析相结合，提供 API 威胁保护。

现代网络应用程序使用并大量暴露 API，这些 API 被用来访问数据和调用应用功能，这创造了一个巨大的和不断增长的攻击面，导致越来越多的暴露的 API 攻击和违规事件。由于 API 通常用于访问数据或调用应用功能，如果敏感数据通过不安全的 API 被泄漏，企业将受到数据安全和隐私法规的处罚。而且 API 安全漏洞防不胜防，一个漏洞可以泄露大量的数据，甚至绕过信息系统防控直接进行危险操作。

所以威胁防护能力就显得格外重要，它主要关注 OWASP API Security

Top 10，需要将正常的 API 使用与蓄意作恶的访问分开，提高 API 安全防护能力。

2.API 安全作为核心

数世咨询认为：

随着数据安全法的正式发布，我国正式进入“以网络安全为基础手段、以数据安全为核心目地的数字安全时代”。我国以全球第二大经济体的身份遨游在数字的海洋中，之前所有的市场和政策环境将不再适合作为数字时代的指导标准。对于数字安全行业来说，市场需求将发生翻天覆地的变化，安全能力作为企业生存的基础，和核心业务融为一体。安全能力将支撑企业业务的可持续发展，并且可独立对外输出，还能从侧面打造企业数字安全感的良好形象。

虽然，传统型 API 安全产品在 API 发展的历程中发挥了巨大的作用，抵御和消除了大部分常规网络攻击，促进了 API 生态的形成。但是，在数字经济和数字生活的环境下，对于 API 技术和模式来说，因其价值承载的影响范围和关键性的深刻变化，单点式、被动型的安全保障方法已经很难再提供强大的前进推动力。

根据数世咨询调研发现，许多企业在 API 安全建设上存在许多共性。例如 WAF 和 API 网关的控制权不归属于同一个团队，很大程度上导致了 API 威胁防护的失效；由诸多第三方供应商提供的部分或全套 API 管理功能，如应用程序开发、集成平台、安全解决方案、B2B 产品等，可能会给企业管理造成混乱；可见性是许多企业缺乏的 API 安全能力，这意味着 API 安全防护的一个关键指标是发现 API，缺乏可见性直接导致了 API 安全无从下手。

从国外 API 安全成熟市场不难看出，解决以上任何 API 安全能力都应该通过平台化的解决方案来体现，而不是一个一次性的工具或扫描器。有效执行 API 安全策略需要一个全生命周期的方法，因为安全风险、漏洞、逻辑缺陷、错误配置等等会在设计、开发、交付和运营的不同阶段出现。

☑ **阿里云 API 安全**

它可以围绕 API 生命周期的各个阶段提供生产力工具，覆盖设计、开

发、测试、发布、售卖、运维监测、安全管控、下线等 API 各个生命周期阶段，是云平台厂商需要为用户提供的必备产品。

它是一种托管式 PaaS 产品，大大提高了 API 管理、运维效率。在安全方面，其可以分布式部署并承载大规模访问、降低处理延迟，可以提供 API 认证、全链路签名、流量控制等多种安全机制，并且可以与 WAF、DDoS 高防 IP 等结合使用，形成全链路 API 安全保障方案。并且快速与阿里云的计算产品、大数据产品、AI 产品、数据可视化产品等深度集成，快速构建业务。

☑ 奇安信可信 API 代理

虽然奇安信这款产品偏传统路线，但是作为其零信任身份安全解决方案中一个重要支点，整合联动了可信接入、可信应用代理、可信访问控制，与其他安全能力并行，共同形成了较为完善的零信任安全防护架构。

API 安全产品自身具备安全接入、动态访问控制、传输加密、流量控制、网络攻击防护、数据攻击防护等标准功能。

☑ 星阑科技 API 安全分析平台

这是国内为数不多的以 API 安全为核心的创新型解决方案，依托 API Runtime Protection 体系，基于 AI 深度感知和强大的自适应机器学习技术来为用户提供 API 安全生命周期安全防护，拥有以下特点：

1) 基于企业级大数据分析平台以及机器学习数据实体识别算法，提供符合国际通用和行业细分标准的敏感数据实体识别与分类分级能力。

2) 针对 API 恶意攻击事件、数据泄露事件、撞库攻击进行实时告警，使企业能够从容应对漏洞攻击、黑客入侵、数据泄露以及账号滥用风险。

3) 通过 AI 驱动的数据模型分析每一次 API 调用，区分正常访问与恶意攻击，自动更新防御逻辑，联动 API 网关实现毫秒级攻击拦截，在不影响业务的可用性与性能的前提下，主动屏蔽 API 攻击向量。

据公开资料显示，该平台的知识产权属于星阑科技。自 2018 年 11 月成立以来，其在 4 轮融资中共筹集了超 2 亿人民币的资金，最新融资是 2021 年 11 月 15 日的 pre-A+ 轮。星阑科技已经在攻防漏洞方面积累了一定经验，并依托大数据分析能力，针对 API 的越权、异常访问、数据泄漏等问题提供

了一种创新性的解决思路。

☑ API 安全本该如此

数世咨询认为：

数字时代的 API 安全产品应该以 API 安全生命周期为线索，在解决协议覆盖、资产梳理以及攻击检测的基础上，通过深度学习的能力，精准描绘出业务逻辑和数据流向。通过对业务流量和数据的学习，整合安全资源，达到攻击预防、攻击阻断以及敏感数据泄漏防护的目的，最终实现 API 运行时防护的安全状态。

数字时代的 API 安全产品已经在全球范围内得到了投资机构、用户和行业的认可，相信通过行业同仁的努力，我国也会诞生出一批 API 安全独角兽，充分保障 API 安全、引领行业发展。

API安全参考框架

根据以上的综合分析，我们不难发现，数字时代的 API 安全产品已经有了逐渐清晰的轮廓。数世咨询认为，API 核心安全能力可以概括如下：

1) 它应该能够发现和识别所有 API、准确锁定风险因素，通过对 API 安全生命周期的监测、检测、测试等手段，收敛攻击面，全面管控 API 安全漏洞以及敏感数据，有效阻断敏感数据泄漏和网络攻击方式。

2) 它应该是一个环境无关和小侵入的平台型产品，整合企业 API 基础设施、API 业务场景中的安全管控能力，发现安全风险后协同联动 API 基础设施和 API 安全管控能力解决针对 API 的数据安全事件和网络攻击事件。

3) 它应该以 AI/ML 的方式来理解 API 业务逻辑，对其学习和风险研判，在运行时精准判定非授权或攻击流量，实现 API 运行时防护的安全状态，最终达到为企业提质增效的目的，预防可能存在的安全风险。

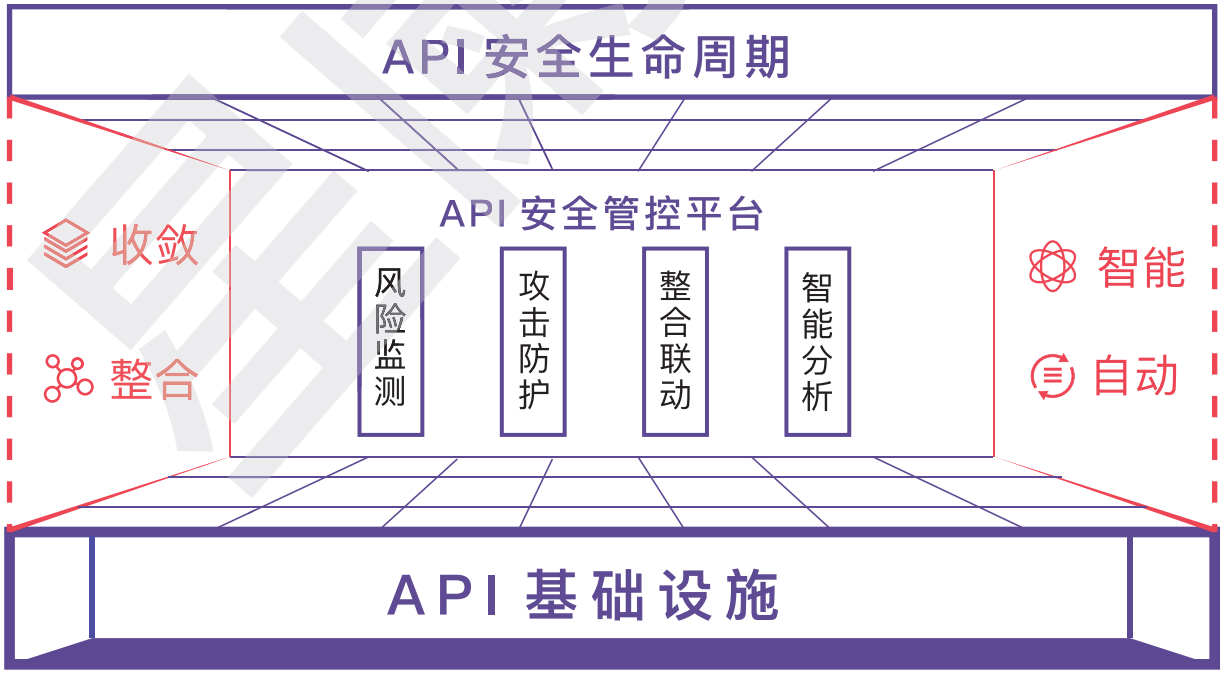


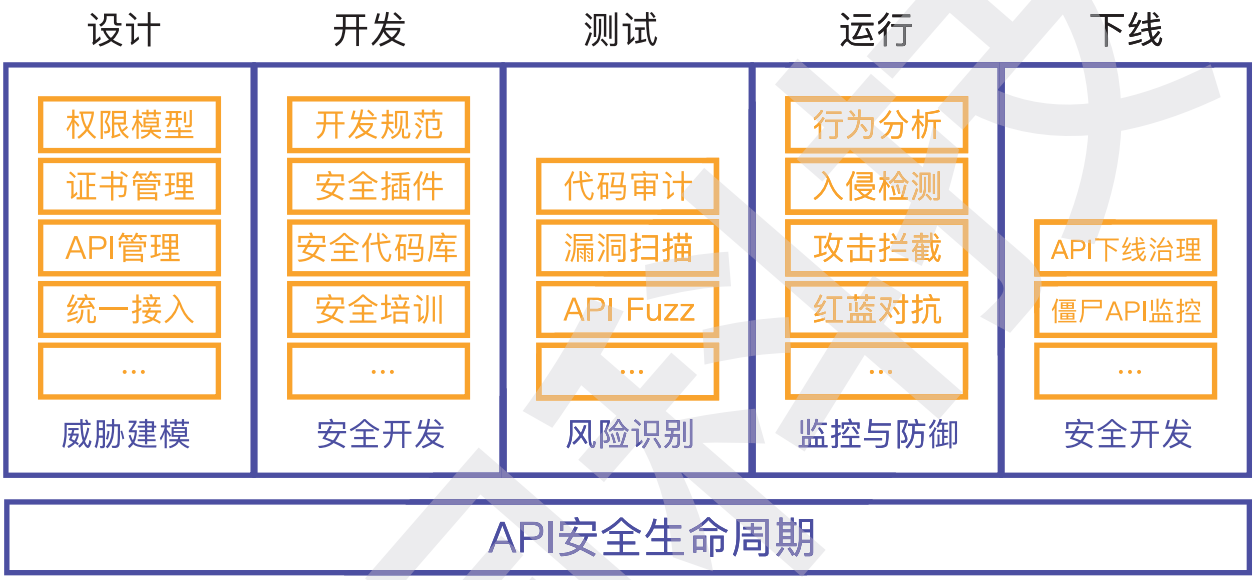
图 4 API 安全参考框架

框架说明

☑ API 基础设施

API 基础设施指企业 API 资源和支持 API 活动的基础网络、计算环境，包括 API、API 网关、API 管理平台、数据总线、容器集群、云平台等。

☑ API 安全生命周期



☑ 风险监测

1) API 清点：安全管控平台要对于每一个 API 进行清晰的记录，与什么类型的数据进行交互，所有者是谁，基础设施中的相关网络、物理资源是谁，以及它属于哪个应用程序或业务部门。这些信息可以从 API 的头部和正文中获取，头部指的是与发送 API 请求和响应有关的元数据，主体指的是被送往和来自 API 的数据。

2) API 识别：持续、自动的识别未被 API 网关或管理产品发现的 API，因为 API 生态复杂，整合的应用程序中和外包开发的产品中都可能出现未知的 API，这些都需要被识别；还要能识别僵尸 API，因为在大规模建设和使用 API 时，在其生命周期中会不可避免的出现多个版本，而旧版本 API 不及时消除或管控的话，这种涉及功能性和数据共享的僵尸 API 就会给企业带来极大的安全风险。

3) 敏感数据监测：能够识别 API 参数和有效载荷中的敏感数据类型，并

适当地标记 API 端点。API 承载了应用各组件间数据的流动，我们需要关注 API 携带了哪些敏感数据、对谁开放、对方如何使用这些数据等问题。企业被爆出数据泄露事件屡见不鲜，除了数据库被攻陷之外，其中很大部分是导致携带敏感数据的 API 鉴权出问题，导致外部攻击者通过不断访问 API 拖取敏感数据。

☑ 攻击防护

1) 攻击阻断：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 安全十大问题中定义的网络攻击。API 安全产品应该能够检测到针对认证的攻击，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。

2) 安全测试：虽然应用程序经历了严格的迭代和测试，但 API 并没有。企业需要对已经投入生产的所有 API 进行持续、积极的测试。因为业务场景的流量、逻辑和功能都在不断变化，这意味着安全态势也在不断变化，而 API 随着业务需求的变化而变化。所以 API 的安全性不应局限于某一时段，应该贯穿于整个安全生命周期。

☑ 整合联动

安全管控平台需要具备与各种业务系统整合联动的能力，应提供与常见的 IT 和 安全系统的整合，在发现网络攻击和数据安全事件时，联合所有资源进行处置。这种整合不应局限于基本的日志保存和数据传输，应智能地对事件进行优先排序，提供可操作的安全警报，并配合 SOC 和 IT 人员的工作流程。这意味着问题可以在被发现时自动分配给适当的团队或系统，而不需要改变工作流程或不同的系统来检查。通常情况下，安全团队需要与 IT、Dev Ops 或业务部门合作来处置风险。

☑ 智能分析

1) 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。

2）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。

报告结语

本报告从 API 的技术应用能力和商业塑造能力两方面阐述了 API 作为数字时代基础设施的重要性，并从其面临的风险、自身复杂度和实际应用情况描述了 API 安全，最后简要介绍了国内外最佳实践者和 API 安全参考框架。

API 安全是一个复杂并且较为新颖的安全研究方向，数世咨询所做的研究和分析大都是在现有技术资料、用户使用反馈和专家访谈的基础上，结合分析师对市场、行业、技术的理解所进行的，可能在某些方面存在值得商榷的地方。在此欢迎广大读者提出宝贵的意见和建议，共同为我国数字安全产业的发展助力。

数世咨询的核心理念为，数字时代、安全共生。希望通过本报告，能够切实解决用户在企业发展过程中出现的关于 API 安全的问题，实现数世咨询的第三方参考价值，帮助企业用户在数字浪潮之中屹立潮头。

数世咨询
Digital World Consulting

第三方中立

- 完全第三方背景
- 独立分析师团队

调研对象

- 700+网络安全企业
- 年均500+深度沟通
- 年均2000+小时访谈时长

服务对象

- 国家、行业监管机构
- 行业客户及用户
- 网络安全产品&服务供应商

服务内容

- 国家、行业智库
- 细分领域等调查研究报告
- 为服务对象提供面对面咨询
- 为产业各方提供资源对接

合作方式

- 各类报告定制
- 年度企业观察列表
- 活动赞助
- 投资FA
- 咨询服务

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《中国网络安全大事记》、《中国数字安全能力图谱》、《中国网络安全能力100强》、《中国网络安全产业统计》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，并与400余家具备原厂能力的安全企业和100余家安全行业领先者企业，以及110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：https://dwcon.cn
联系邮箱：dw@dwcon.cn

数世咨询官方微信

数字时代　安全共生