数世咨询市场洞察报告

《民营第三方网络安全服务》

北京数字世界咨询有限公司

2023年11月

前言

近年来，在“安全合规”与“实战化需求”两大驱动力的共同助力下，数字安全行业迎来快速发展期。安全设备、安全工具、安全平台等各类安全产品在不同行业、不同规模的机构用户中得到广泛部署。

然而，数字安全的碎片化、动态化等本质决定着，“服务化”成为贯穿于机构用户安全咨询、安全建设、安全运营全流程的刚需，加之国内不同行业间安全发展不均衡、安全团队水平参差不齐、安全人才紧缺等因素，导致本应与安全产品相配套的安全服务明显滞后，机构用户中仍存在着大量的安全服务需求。

需求方既包括安全建设水平相对高一些的大型关基行业用户（实战化需求），也包括处在安全建设相对初期的行业用户（合规需求）。前者的需求大部分由提供安全产品的安全企业配套提供，后者则由区域型或行业性的专业安全服务提供商来满足。提供的安全服务有信息系统等级保护、商用密码应用安全评估、信息系统安全评估，以及安全咨询、安全运维、安全监理等，分别满足不同用户的实战化安全需求与安全合规需求。

伴随信息安全测评与认证、信息安全运营等服务需求近年来的快速增长，2022 年发布的新版的国家标准《GB/T 30283-2022 信息安全技术 信息安全服务 分类与代码》在传统分类信息安全咨询服务、信息安全培训服务等基础上，扩展增加了信息安全测评与认证、信息

安全运营等服务分类，这无疑会更好的规范和引导信息安全服务市场。

在上述背景下，经过多年发展，行业中已经涌现出一批优秀的第三方网络安全服务提供商，形成了一个“既传统又创新”的细分市场——第三方网络安全服务。本报告将针对这一细分市场进行调研，尝试梳理其市场现状，洞察其市场趋势。

市场现状

目前，国内提供服务的安全企业众多。大致分为三类：第一类是国家各职能部门、科研院所或大型央国企下辖的安全服务机构，即业内俗称的“国家队”；第二类是头部综合型安全企业，此类企业大部分已经上市，在各地组建有安全服务团队，为各地机构用户提供服务支撑，其服务的特点是，大部分服务是与该厂商自研的安全产品配套提供的；第三类是以第三方网络安全服务为主营业务的民营企业，此类服务商以网络安全认证、检测和风险评估为主营业务，辅以配套的安全测试、安全运营和安全咨询等服务，一般具有明显的地域特征，在当地有更加稳定的安全服务团队，但也有极少数企业在全国范围内开展业务。

本报告主要针对第三类民营企业进行市场调研与统计。此类企业不同于前两者。首先其身份属于民营企业；其次其交付的服务不与某一家、两家安全企业的安全产品绑定；最后，其服务内容以等保、密评、安全评估与测试等为主，满足的是大部分机构用户的合规类需求，

目标是提升国内整体安全行业的“底线”。

服务内容

本报告所描述的民营第三方网络安全服务包括信息安全咨询、信息安全工程监理、信息安全测试、信息安全风险评估、信息安全运营以及等级保护测评、密码测评服务，不包括安全集成、安全培训、安全意识教育等服务。

基于2022年发布的新版的国家标准《GB/T 30283-2022 信息安全技术 信息安全服务 分类与代码》，各项服务定义如下。

服务名称	服务内容
信息安全规划咨询	信息安全规划咨询主要是针对需方信息系统及其支持的业务和管理的安全需求,由供方结合需方投资预算、信息安全现状以及发展趋势,基于人员利用资源、技术,通过规定的过程提出需方安全规划目标。从管理、技术两个维度设计规划内容以形成一套指导性文件,系统指导需方信息安全建设，满足其可持续发展的需要。信息安全规划咨询通常涉及多学科知识、工程实践经验、现代科学和管理技术,为信息安全资源开发利用、工程建设、人员培训、管理体系建设、技术支撑等方面提供支持。
信息安全设计咨询	信息安全设计咨询主要是针对信息系统的安全防护需求,由供方落实需方的安全规划,设计总体安全策略,制定信息安全建设方案和实施方案,并在此基础上形成安全策略、安全技术体系结构、安

	全管理体系结构等的设计,指导需方信息安全防护具体实现。信息安全设计一般可分为顶层设计、概要设计和详细设计等不同的服务交付物。
信息安全管理体系咨询	信息安全管理体系咨询主要是针对需方信息安全管理体系需求,由供方结合需方的需要和目标、安全要求、所采用的过程、规模和结构,通过确定信息安全管理体系范围和方针、明确责任、权限和角色,采用风险评估的方法规划管理体系建设任务并落实,实施内部审核与管理评审等过程,协助需方建立、实现、维护、并持续改进信息安全管理体系。信息安全管理体系是组织的过程和整体管理结构的一部分并集成在其中,涵盖相关标准要求的文件化信息，应阐述被保护的资产、风险管理的方法、控制目标及控制方式和需要的保证程度。
信息安全工程监理	信息安全工程监理主要是针对需方各类信息系统工程中涉及信息安全的工程活动,由具有相关资质的监理单位(供方)根据需方委托,在工程建设的规划设计、部署实施(招标、设计、实施、验收)各阶段实施控制和管理,提供相关建议和意见,确保实现各阶段的监理目标和完成监理内容。信息安全工程监理还可以包括对信息系统运行维护阶段的信息安全服务进行监理。
信息安全测试	信息安全测试主要是针对信息系统、软硬件产品等被测对象的安全属性,由供方在特定的测试环境下,根据需方授权,按照测试准备、测试实施、测试分析、测试结果反馈等工作流程，选择适用的方法/工具,动态分析测试数据发现被测对象存在的安全隐患,验

	证被测对象安全保障措施的符合性及有效性。提出安全整改建议。信息安全测试通常包括信息系统安全测试、APP 安全测试、漏洞安全扫描、基线配置核查、渗透测试、源代码审计等。信息安全测试工具应符合相关国家标准要求,确保可靠性和安全性。
信息安全风险评估	信息安全风险评估主要是针对业务、信息系统、基础网络和平台、数据资源等被评估对象,由供方确定风险评估的工作形式,按照风险评估流程,覆盖风险评估准备、资产识别、威胁识别、脆弱性识别、已有安全措施确认、风险分析、风险处理等环节,对所面临的风险进行识别、分析和评价,制定和提出抵御风险的安全策略和整改措施。信息安全风险评估通常贯穿被评估对象的规划、设计、实施、运行、废弃各生命周期阶段。
信息安全运营服务	信息安全运营旨在确保组织的信息系统和数据得到有效的保护和管理。可以包括信息安全监测、信息安全检查、威胁信息共享、信息安全分析、信息安全报送、恶意代码防范和处理、信息安全应急响应、信息安全演练、信息安全调查取证、信息安全加固、信息安全审计等。
等级保护测评	等级保护测评主要是针对需方的网络安全等级测评需求,由具有服务资质的测评机构(供方)根据需方委托,依据国家网络安全等级保护制度规定,按照有关管理规范和技术标准,采用相关测评手段,遵从一定的测评规程结合等级保护对象的安全级别,对非涉及国家秘密的网络安全等级保护对象进行检测评估,并出具等级保护测评报告,协助需方评判是否达到特定级别安全保护能力。等级保

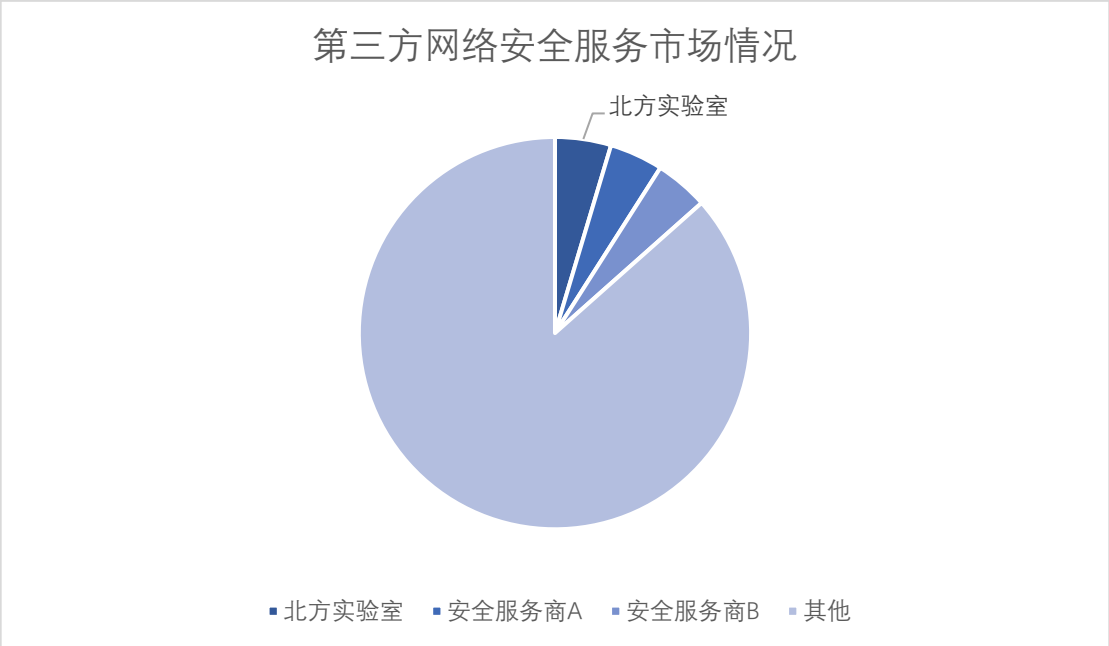
	护测评包括单向测评和整体测评,其中单向测评包括物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、安全策略和管理制度、安全管理机构和人员、安全建设管理和安全运维管理等方面。
密码测评	密码测评即商用密码应用安全性评估主要是针对需方使用密码的信息系统,包括相关配套密码产品、通用设备、人员、制度文档等,由具有相关资质的供方根据需方委托,根据已通过评审的密码应用方案、有关管理规范和技术标准,按照测评准备、方案编制、现场测评、分析与报告编制等过程开展测评,对密码应用的合规性、正确性和有效性等进行评估，以规范密码应用和管理。密码测评通常包括物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、管理制度、人员管理、建设运行和应急处置等方面。

市场规模

根据《中国数字安全产业年度报告(2023)》中统计的数字，2022年度国内数字安全市场规模为981.2亿元，其中安全服务收入约占总收入的12%。

据数世咨询不完全统计，2022年度民营第三方网络安全服务的市场规模约为50亿元，约占国内安全服务收入的42%，其中北方实验室市场占比位居第一。

其中主要头部企业（按照营收 1 亿元以上计），收入在 1 亿至 2 亿左右规模不等，差距并不明显，且主要头部企业营收之和占比仅占整个民营第三方网络安全服务市场规模的 20%，市场格局总体较为分散。



注：需要再次说明的是，本章节及图表中“第三方网络安全服务商”指以等保、密评、安全测试与评估等安全服务为主营业务的民营企业。相关市场规模统计，也仅以上述服务提供商为主要统计对象。“国家队”、以安全产品为主营业务的安全企业均不在本统计范围内。

洞察

第三方安全服务市场具有明显的区域性特点

在调研中我们发现，民营第三方网络安全服务市场具有明显的区域性特点，即某个区域的第三方网络安全服务大多集中在两到三家规

模较大的服务提供商手中，同时这两到三家服务提供商的大部分业务也都集中在该区域。不同区域间的第三方安全服务供需间很少有合作交集。

第三方安全服务的核心基础在于资质的更新与维护

等级保护、商用密码应用评估以及新近出现的数据安全相关安全服务，需要服务商具备相应的安服资质。资质对应的是服务商对法律法规政策合规的解读能力，以及与之对应的安全技术服务能力。也就是说，需要服务商第一时间“吃透”相关政策所对应的技术落地执行点，例如数据出境等新形势新要求。资质的更新与维护，背后是服务商优质的安全能力，两者是一脉相承的。

第三方安全服务的核心竞争力是专业化、技术驱动

就目前行业现状来看，虽然有等保工具箱等标准化检测产品，但第三方安全服务仍然需要依靠大量的专业技术人工参与，特别是有丰富经验的安全工程师参与项目后会显著提升安全服务效果的上限。通过持续技术创新不断提升行业竞争力，如采用自动化、智能化的服务工具对于提升安全服务效果、降低服务成本效果显著。不局限特定某类业务，不断扩展信息安全服务业务线，甚至打造全过程第三方服务能力，在碎片化的服务市场中更加具有竞争力。因此，未来一段时间内，如何加强企业管理、培育良好的企业文化吸引和培养专业人才、持续进行核心技术研发创新、打造全过程第三方服务能力，从而留住已有高端人才，培养更多高端人才，是第三方安全服务提供商核心要

关注的问题，也是其核心竞争力的所在。

传统的安全合规需求将向“持续合规需求”发展

近几年，《网络安全法》、《密码法》、《个人信息保护法》、《数据安全法》、《关键信息基础设施安全保护条例》、《商用密码管理条例》等一系列法规陆续颁布实施。大数据、人工智能为代表的信息技术日新月异，与此同时，网络攻击、网络窃密、网络诈骗呈现高发态势，网络安全的风险正在被技术不断放大。实战化、体系化、常态化，不仅限于关基行业，千行百业的安全合规需求，也需要向三化六防靠拢，因此传统的安全合规需求将逐步向“持续合规需求”发展。同时，随着国际形势的变化，信息技术应用创新产业作为实现助力数字技术领域科技自立、保障国家安全的必由之路，已成为国家战略。新的需求需要新的服务交付能力，创新的方向就在于，服务提供商如何将一年几次的安全测试、评估、适配验证等人工服务交付方式，转变为持续满足合规要求的平台化安全服务能力交付。人的参与度降低，避免人为因素的服务不一致性；自动化、工程化的程度增加，合规的持续性与服务质量的一致性都能得到保证。

（End）

主笔分析师：刘宸宇

勘误与沟通：liuchenyu@dwcon.cn

数世咨询
Digital World Consulting

第三方独立

- 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

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

数字安全领域独立第三方调研咨询机构