2018年中国信息安全行业分析报告-市场深度调研与发展前景研究

报告大纲

观研报告网
www.chinabaogao.com

一、报告简介

观研报告网发布的《2018年中国信息安全行业分析报告-市场深度调研与发展前景研究》涵盖行业最新数据，市场热点，政策规划，竞争情报，市场前景预测，投资策略等内容。更辅以大量直观的图表帮助本行业企业准确把握行业发展态势、市场商机动向、正确制定企业竞争战略和投资策略。本报告依据国家统计局、海关总署和国家信息中心等渠道发布的权威数据，以及我中心对本行业的实地调研，结合了行业所处的环境，从理论到实践、从宏观到微观等多个角度进行市场调研分析。

官网地址：http://baogao.chinabaogao.com/xixinfuwu/328448328448.html

报告价格：电子版: 7200元　纸介版：7200元　电子和纸介版: 7500

订购电话: 400-007-6266 010-86223221

电子邮箱: sale@chinabaogao.com

联 系 人: 客服

特别说明：本PDF目录为计算机程序生成，格式美观性可能有欠缺；实际报告排版规则、美观。

二、报告目录及图表目录

信息安全高端人才主要集中于大的安全厂商以及军队所属的研究机构，其共同特点是数量稀少、聘用成本较高、具有国防网络装备生产资质的企业普遍对其核心技术人员具有较强的管控能力。这使得新进入者在人才稀缺的情况下，无法在短期内突破研发领域中的技术难关，从而难以形成自身的技术或差异化优势。

（四）影响行业发展的有利和不利因素

1、有利因素

（1）信息安全已上升至国家战略的高度，行业面临良好政策环境，是行业快速成长的推动因素。

近年来，全球信息安全问题迭出，迫使政府和军队进一步重视网络信息安全问题，不断加大相关方面的投入。2013年6月，美国前中央情报局（CIA）雇员斯诺登披露了美国国家安全局（NSA）实施的“棱镜”项目，NSA 和联邦调查局（FBI）直接进入美国网际网路公司的中心服务器里挖掘数据、收集情报。

该事件引爆国家、企业和个人对信息安全的重视。近年来，信息安全、云计算和大数据产业获得了国家战略层面的重视和支持。

2014 年中共中央网络安全和信息化领导小组成立；2015 年《网络安全法》发布，体现出网络安全对维护国家利益、推动信息化发展的重要作用，有助于提高全社会和各行业对网络安全的重视程度。信息安全对国家安全、经济发展的保障作用得到广泛认可，关键信息基础设施和政府信息系统普遍加强了网络安全防护体系的建设。面对日趋复杂的国际政治军事环境，国家和军队不断加大信息安全建设投入，这必将为国防网络通信和信息安全相关企业带来新的机遇、挑战和发展空间。

国家一直强调要健全信息安全保障体系，增强信息安全保障能力。2013 年，《中共中央关于全面深化改革若干重大问题的决定》中提到了确保国家网络和信息安全。2015 年8月，《国务院关于印发促进大数据发展行动纲要的通知》要求健全大数据安全保障体系，加强大数据环境下的网络安全问题研究和基于大数据的网络安全技术研究。本土信息安全行业在国家战略和相关政策的积极促进下，将迎来发展的重要契机与机遇。当前国家已经逐步出台一些可落实到操作层面上的政策，未来更多的细化政策有望出台，加速信息安全需求落地，全面利好产业发展。

（2）随着云计算和大数据技术不断发展，军队所面临的信息安全威胁不断演化，迫切需要安全防护体系和产品服务进行更新换代，市场空间可期。

随着军队的组织架构日趋完善，各种类型的安全设备、安全数据越来越多，传统的分析能力明显不足。为应对以高级持续威胁（APT）为代表的新型安全威胁，安全防护系统需要储存和分析更多的安全信息并且更加快速地做出判定和响应。这需要传统的安全防护体系做出变革，安全云和客户侧安全防护设备分工合作，在安全决策智能性、协同性和运营效率方面实现明显的提升。军事信息安全领域具备很强的对抗特征，安全防护体系、防护技术和产品、防护策略规则等都需要持续、及时升级换代，以应对高技术战争条件下进行信息化军事

斗争的需要。

（3）军队信息化建设和信息战的发展，云计算、大数据、智能终端、移动通信等新信息技术的不断涌现，极大地推动数据流量的增长，带来新的网络安全产品需求，是驱动国防网络信息安全行业加速发展的基本因素。

信息化技术发展日新月异，云计算、大数据、智能终端、移动通信技术已广泛应用于国防信息化建设，随之而来的信息安全问题将更加突出，对信息安全产品提出了更为复杂的要求，催生云安全等新的信息安全应用领域。

中国军队的信息化建设正处于信息化全面发展的重要阶段。近年来，国防信息系统栅格化发展趋势明显，信息系统与指挥控制、武器平台及其他终端的融合不断加深。这一趋势对支持云计算、大数据的网络安全平台从功能上和性能上都提出了完全高于传统平台的新要求。

在国防领域，任何信息的传递都必须首先保证保密和安全，信息安全出现问题很可能导致严重的国家利益损失，因此，所有涉密网络都需要安全设备。此外，随着智能终端、移动通信设备功能性能的提升以及现代战争和军队办公对通信的机动性、实时性、便捷性提出更高要求，智能终端和移动通信设备在日常办公、作战指挥中的应用快速发展，其安全产品与技术应用具有很大的潜力和应用前景。

（4）自主可控的安全保密平台需求不断增长以及国防网络信息安全产品核心软硬件国产化都推动了更新换代的新需求。

信息安全已成为左右国家政治命脉、经济发展、军事强弱和文化复兴的关键因素。构建完整、可靠的信息安全保障体系是一个复杂的系统工程，而自主可控的技术和产品则是信息安全的基石。

安全装备是军事网络安全和信息安全的核心环节，应用范围和数量呈逐年增长的态势。信息安全已上升到国家战略的高度，未来国家将通过政府采购或政策扶持等方式逐渐实现基础软硬件和重要IT 服务的国产化替代。军队也已明确要求军工安全产品必须采用国产芯片、软件，实现自主可控。因此，信息安全产品核心软硬件国产化将带来自主可控的信息安全装备平台的巨大需求。

（5）国防和军队体制改革的不断深入，为民营军工企业的发展提供了巨大的发展空间。

随着科技产业革命和新军事变革的迅猛发展，国防经济与社会经济、军事技术与民用技术的界限趋于模糊，军民融合式发展已成为顺应世界新军事变革发展的大趋势。

新的“军改”政策下，部分科研院所也列入调整范围，这将意味着大量科研及装备生产任务将不再由军队承担，国防科研单位把工作重心放在了装备总体论证规划方面，大量装备的研制和生产交由地方工业部门和企业承担。

未来，随着军民融合的深度推进，具有强大研发实力、优秀管理团队、良好市场声誉的民营企业将迎来巨大的成长空间。我国政府正逐步有序向社会资本开放军工市场，这为我国

国防网络通信和信息安全相关企业带来了新的机遇和发展空间，整个行业面临较好的发展前景。

2、不利因素

不利因素

产业配套体系有待完善

虽然近几年我国信息安全市场快速发展，但与民用信息安全领域相比，国防网络信息安全领域产业链条不够完善。同时，由于信息安全产业整体发展程度有限，导致我国信息安全企业在高端人才吸引和新产品研发投入方面力度较为有限。因此，国防网络信息安全行业的发展在一定程度上依赖于产业链整体的发展和提升。

专业人才缺乏

信息安全产品的研制融合多学科的高精尖技术，对人员的技术要求高，人才培养周期长，导致了国内信息安全产品的研发人才队伍建设不能充分满足行业发展的需求，同时我国信息安全行业起步较晚，经验丰富、技术能力强的专业技术人才和管理人才较缺乏。随着国防建设的需要，国防网络信息安全产品市场规模稳步扩大增长，专业人才的缺乏问题矛盾将会更加突出。

（五）行业未来的发展趋势

移动互联网、物联网、云计算等技术的快速发展，一方面使得军事斗争所面临的信息安全形势愈发严峻，近年来频繁出现的信息安全事件给国家安全和军队的正常运作带来了大量的损失，信息安全愈发受到政府和军队的高度重视；另一方面，新技术也为维护国防网络信息安全提供了新的手段，从而也为国防网络信息安全行业带来了新的市场发展空间。

1、国防网络信息系统的合规及安全管理产品形成新的市场增长点，信息安全在国防网络信息系统中的核心战略地位和重要性日渐增强

随着国防和军队改革的逐步推进，与国防网络信息安全相关的政策和规范不断出台，国防网络信息系统对类似于检查评估、上网行为管理、安全审计等产品的需求持续增加。此外，在早期的安全加固、系统评估、值守呈现普遍化的情况下，国防网络信息系统在运行和维护过程中对于业务安全评估、安全度量、软件安全生命周期、SaaS（软件即服务）化安全的需求不断增强，形成了新的市场增长点。随着国家和行业政策、监管的不断加强，与国防网络信息系统相配套的合规和安全管理产品也会不断普及，从漏洞扫描延伸出的漏洞管理产品、基线核查产品和安全审计产品等都有较好的市场前景。

2、创新性的安全运维服务或云安全服务会成为国防网络信息安全领域的一个新兴增长点

单纯依靠产品无法彻底解决用户安全问题，用户更加关心厂商如何帮助他们解决问题。随着基于云计算的信息安全技术的发展，军队信息化建设所带来的信息安全意识的提升以及军工产品领域向民营企业的不断开放，未来安全运维服务以及云安全服务等创新性的服务会为军队用户提供更加完善、及时的服务。

3、信息安全产品向多功能化方向发展，集成的安全解决方案将成为用户首选

由于军队信息系统巨大的规模及其拓扑的复杂性，许多功能单一的信息安全产品越来越无法满足军队客户的信息安全保障需求。这将促使国防网络信息安全产品将向多功能化方向发展。

同时，由于国防网络信息系统待命时间长，担负的责任重大，因此需要尽量减少系统维护与调试的时间，对于持续性出现的新型安全威胁，军工客户普遍期望安全信息系统对于未来一段时期内可能出现的信息安全威胁提供一个预反应机制，以便能够全面解决军队所属组织机构安全管理、国防网络信息安全防护以及主动应对不断升级的威胁。

观研天下发布的《2018年中国信息安全行业分析报告-市场深度调研与发展前景研究》内容严谨、数据翔实，更辅以大量直观的图表帮助本行业企业准确把握行业发展动向、市场前景、正确制定企业竞争战略和投资策略。本报告依据国家统计局、海关总署和国家信息中心等渠道发布的权威数据，以及我中心对本行业的实地调研，结合了行业所处的环境，从理论到实践、从宏观到微观等多个角度进行市场调研分析。

它是业内企业、相关投资公司及政府部门准确把握行业发展趋势，洞悉行业竞争格局，规避经营和投资风险，制定正确竞争和投资战略决策的重要决策依据之一。本报告是全面了解行业以及对本行业进行投资不可或缺的重要工具。观研天下是国内知名的行业信息咨询机构，拥有资深的专家团队，多年来已经为上万家企业单位、咨询机构、金融机构、行业协会、个人投资者等提供了专业的行业分析报告，客户涵盖了华为、中国石油、中国电信、中国建筑、惠普、迪士尼等国内外行业领先企业，并得到了客户的广泛认可。

本研究报告数据主要采用国家统计数据，海关总署，问卷调查数据，商务部采集数据等数据库。其中宏观经济数据主要来自国家统计局，部分行业统计数据主要来自国家统计局及市场调研数据，企业数据主要来自于国统计局规模企业统计数据库及信息安全交易所等，价格数据主要来自于各类市场监测数据库。本研究报告采用的行业分析方法包括波特五力模型分析法、SWOT分析法、信息安全T分析法，对行业进行全面的内外部环境分析，同时通过资深分析师对目前国家经济形势的走势以及市场发展趋势和当前行业热点分析，预测行业未来的发展方向、新兴热点、市场空间、技术趋势以及未来发展战略等。

【报告大纲】

图表详见正文（GYWW）

详细请访问：http://baogao.chinabaogao.com/xixinfuwu/328448328448.html