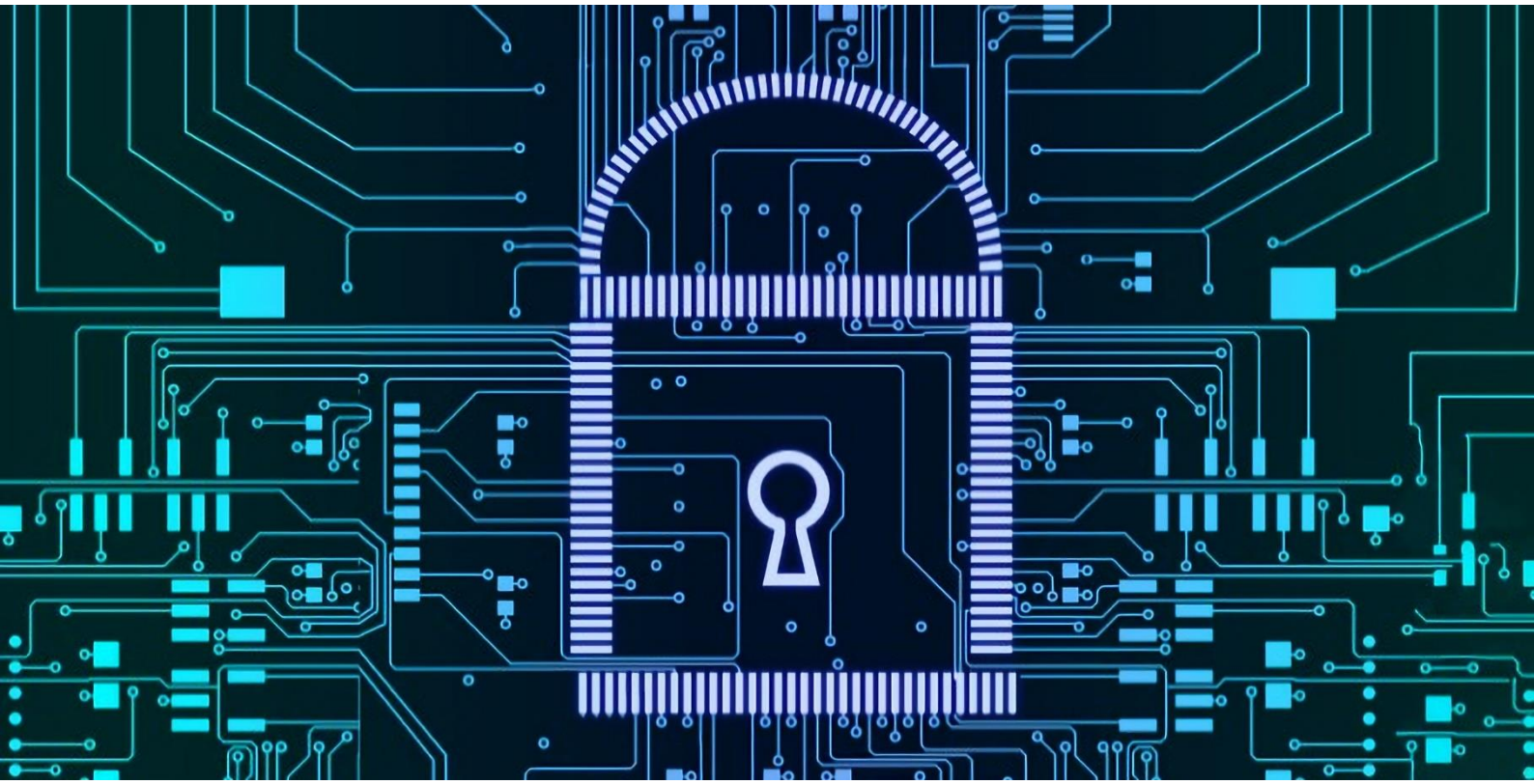
数世咨询
Digital World Consulting

信创安全市场指南



数世咨询
Digital World Consulting

信创安全市场指南

数字安全的三个元素分别为，安全能力、数字资产和数字活动。数字资产是安全能力的保护对象，数字活动是安全能力以及数字资产的服务对象，而数据安全则是三元论的核心目标。对于这四者关系的深度理解和相关技能掌握是做好数字安全工作的关键。

数字安全能力模型研究的基础，来自于数世咨询 2020 年首次提出的"网络安全三元论"。三元分别为，网络攻防、信息技术和业务场景。

随着数据成为第五大生产要素为典型标志的数字时代来临，“网络安全三元论”在 2022 年进行了更新迭代升级为“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”，以适应我国数字中国建设的进程。

数世咨询作为国内独立的第三方调研咨询机构，为监管机构、地方政府、投资机构．网安企

业等合伙伙伴提供网络安全产业现状调研，细分技术领域调研、投融资对接、技术尽职调查、市场品牌活动等调研咨询服务。

报告编委

主笔分析师 **陈发明**

首席分析师 **李少鹏**

分析团队：**数世智库** 数字安全能力研究院

目　录

1 前言

信创（信息技术应用创新）产业是国家安全稳定和经济社会发展的重要组成部分，也是数字化转型、提升产业链发展的新动能。信创产业涉及 IT 基础设施、基础软件、应用软件以及信息安全等领域，这些领域的产品和服务共同构成了信创产业的完整产业链和生态体系。多家调研机构的调研显示，目前信创产业已达到万亿规模。

信创安全是指在信息技术创新发展的背景下，为保障国家信创生态系统的信息安全和网络安全而提出的一个重要概念。近年来，信创安全市场进入快速增长通道，发展方向逐步明确，其市场空间巨大。数世咨询在交流过程中，了解到许多产品供应商、甲方用户以及投资机构对信创安全市场和相关产品方案有高度关注。

为了客观真实地反映信创安全市场及应用情况，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《信创安全市场指南》，报告从信创安全定义、市场规模、能力企业、场景应用、挑战机遇、发展趋势、应用案例等多个方面对信创安全市场进行分析。以供业内人士参考。

勘误或进一步沟通，请联系主笔分析师：陈发明 chenfaming@dwcon.cn

2 关键发现

- ✓ 那些尽早开始信创适配，投入资源积极进行技术攻关的厂商，已经在信息安全市场中获得先机。
- ✓ 2023 年信创安全市场规模约为 50 亿元，预估到 2027 年信创安全规模能到 166 亿元。
- ✓ 安全厂商从 2020 年到 2023 年的信创安全营收在持续增加，复合增长率达到 35%，显示出信创安全市场的巨大成长潜力。
- ✓ 信创安全产品在不同行业的应用分布：政府（29.8%），国防（24.5%），金融（10.1%），运营商（9.1%），其它行业（26.5%）。
- ✓ 当前最需要的信创安全产品 TOP3：边界安全（29.9%）、终端安全（22.5%）、安全管理（18.2%）。
- ✓ 信创安全骨干企业走在国产化适配队伍的前列，产品的国产化率大多达到 70%以上，个别厂商超过 85%。
- ✓ 受政策推进、信创产业发展、以及国产化适配技术困难度的影响，信创安全细分领域仅有少数安全企业针对国产化推进做好了准备。
- ✓ 信创安全不仅仅是“国产替代”，信创安全产业的发展需要安全厂商与上下游产业伙伴紧密合作，共建信创生态。

3 市场概况

3.1 概述

自 2013 年开始的"党政电子公文系统"的安全可靠升级发展到现在万亿规模的信创产业，经过多年的发展和实践，目前已逐渐形成"2+8+N"战略布局（注1），这里 "2"指的是党政，"8"指的是金融、电信、石油、电力、交通、航空航天、医疗和教育八大关键行业，"N"则指其他行业。2019 年以来，随着国产化替代从党政开始扩大到更多行业，我国信创产业进入发展快车道。

图例：信创产业

信创产业包括基础硬件、基础软件、应用软件和信息安全等几大领域，其中“信息安全”即是本报告所调研和讨论的范围，业内称为“信创安全”。

信创安全要实现两个安全目标：一个是通过使用国产化的软硬件安全产品替代核心部件非国产的安全产品，实现安全产品的自主可控；另一个是为信创软硬件环境提供专门的安全防护、应对安全风险。可以说“信创安全”对整个信创产业的发展具有关键的战略

[1] "2+8+N"规划路线是中国信创产业发展过程中形成的一个战略布局，其具体的出处并非单一文件或报告，而是在国家政策的持续推动和行业实践的不断探索中逐步明确和推广的。

意义。

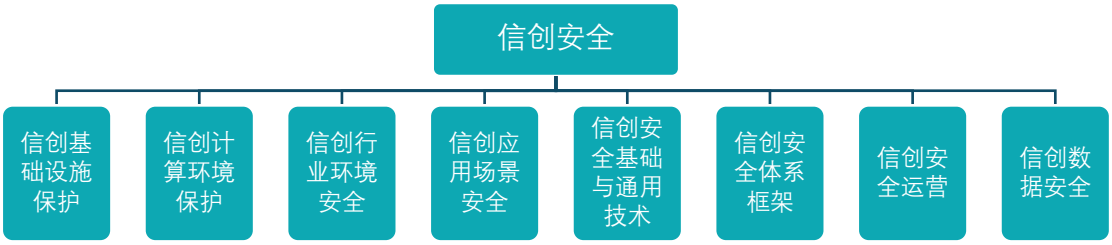
3.2 定义与范围

基于前文所述信创安全要实现的两个目标，数世咨询给信创安全定义如下：

信创安全，即信息技术应用创新（信创）安全，是一套综合的安全保障体系，旨在通过国产化软硬件安全产品及相关服务，确保信创系统在面对病毒、黑客攻击、数据泄露等安全威胁时的稳定性和安全性。

我国信创安全产业尽管起步晚，但起点并不低，站在传统安全产业发展基础之上，信创安全继承发展了信息安全关键技术及安全理念。当前的信息安全实质上已经演变为“以网络安全为基础手段，以数字安全为核心”（注[2]）的数字安全防护体系。参照数字安全体系分类，信创安全体系可细分为：信创基础设施保护、信创计算环境保护、信创行业环境安全、信创应用场景安全、信创安全基础与通用技术、信创安全体系框架、信创安全运营、信创数据安全八大分类。

[2] 数世咨询《数字安全蓝皮书》（2024）



图例：信创安全体系

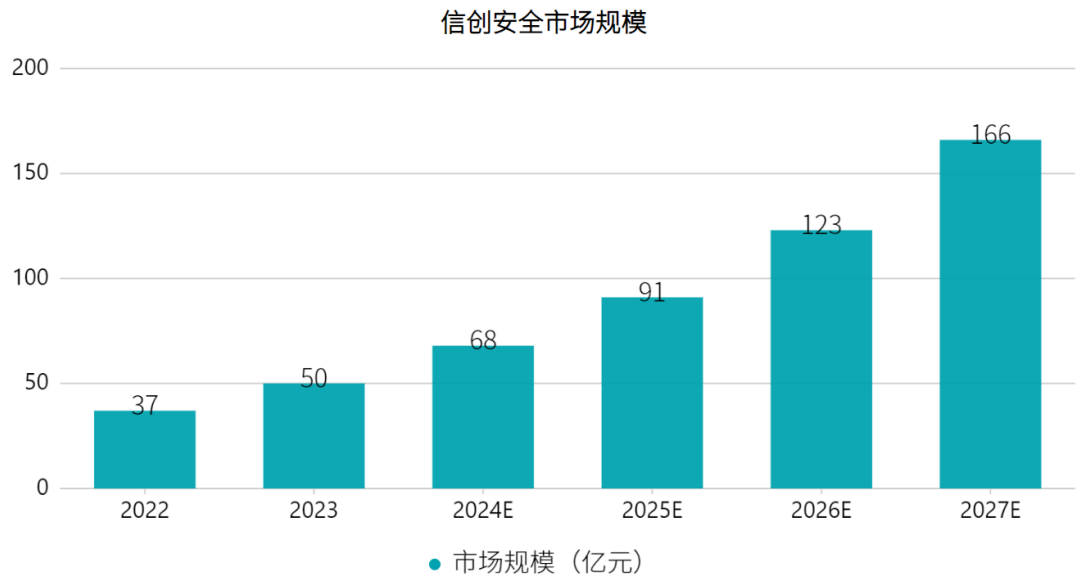
3.3 市场规模

多家调研机构的数据显示，目前信创产业已达到万亿规模，按信息安全投入占 IT 投入 3%的比例估算，信创安全市场规模应不少于 300 亿，然而数世咨询调查统计发现，2023 年信创安全实际规模距估算值相去甚远，仅约 50 亿元（注[3]）。

从安全厂商近三年来的营收数据来看，信创安全产品收入持续增加，复合增长率平均达到 35%，预计到 2027 年信创安全市场将达 160 亿规模：

[3] 数据误差一：数据基于对 20 余家营收过亿的安全骨干企业、十余家细分领域代表企业 2023 年的信创安全产品营收统计，与总体市场规模占比反向计算得出，存在比例估算不准的误差。

数据误差二：部分厂商反馈因无法精确分拆项目中信创产品的具体营收，存在部分原始数据统计上的误差。

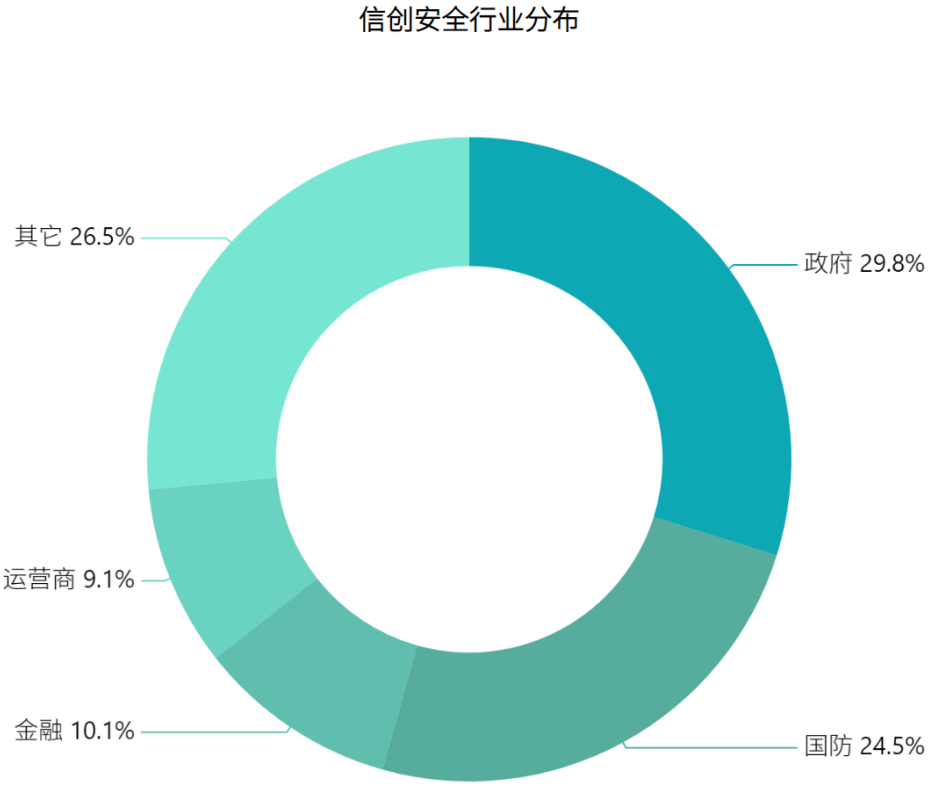


图例：信创安全市场规模

3.4 行业分布

信创安全产品在不同行业的应用状况与国家政策导向高度匹配，在政策推动下，党政机关作为信创引导力量，在推动国产化项目上的需求最为迫切，目前仍是信创安全第一梯队。金融行业具有较好的数字化基础，又是社会经济的核心领域，金融系统积极执行信创政策，很早就开始国产化替代的工作。运营商是关键信息基础设施建设的中坚力量，能够投入大资金进行规模化安全建设，金融和运营商位于信创安全发展的第二梯队。能源、石油、交通、电力、教育、医疗等行业也正在进行信创政策和信创安全监管推进，处于第三梯队。

2023 年不同行业信创产品应用分布比例：政府（29.8%），国防（24.5%），金融（10.1%），运营商（9.1%），其它行业（26.5%）。



图例：信创安全产品行业分布

3.5 信创安全产品

尽管当前整个信创安全产品体系框架已经基本形成，但受限于信创产业的整体发展状况及市场需求情况，跟传统的安全产业相比，信创安全发展相对滞后，具体体现在安全产品与信创环境的适配周期比较长，部分细分领域尚无国产化产品，难以形成体系化安全解决方案。目前信创产品更多的集中在端点安全、边界安全、网站安全、云安全、数据访问安全、日志审计、身份认证和安全管理等几个细分领域。

信创安全产品的应用分布与信创产业整体的发展状况息息相关。

在信创推进的初始阶段，以 PC 终端和应用服务器的国产化替代为主，终端安全是刚性的需求，终端安全类主要产品有终端杀毒、主机监控、终端检测与响应（EDR）等。

随着信创 IT 系统建设逐步完成，需要满足边界安全和安全管理等相应的合规要求。边界安全主要产品：防火墙、上网行为管理、隔离网闸、抗 DDoS、入侵检测与防御（IPS/IDS）、VPN 等。

数据安全国产化主要集中在特定行业，如金融和军工等，其他行业的数据安全需求还没大范围释放。信创数据安全产品主要有：数据防泄漏、敏感数据管控以及数据管理平台。

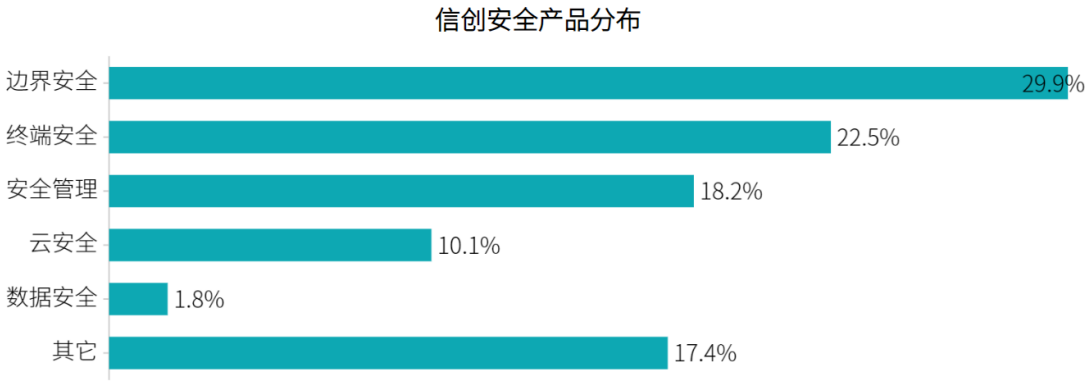
工业软件和工控系统的国产化仅有部分厂商尽早进行了适配工作。信创工控安全产品主要有：工控网闸、工业防火墙、边界审计系统、数据交换审查审批系统等。

应用安全的产品需求主要集中在 WEB 安全、邮件安全、漏洞扫描、办公安全等领域。

国产密码作为信息安全领域的基石性技术，目前已建立起一套完善的算法体系，基于国产密码的各类加密、认证和数字签名等产品实际表现可靠稳定，已大量应用于国产化信创环境。主要产品有：密码机、数字证书、签名验签服务器等。

其它信创安全信创安全产品还有：浏览器安全访问，软件开发安全、信创靶场、安全运营管理等。

信创安全产品应用分布：边界安全（29.9%）、终端安全（22.5%）、安全管理（18.2%）、云安全（10.1%）、数据安全（1.8%）、其它（17.4%）。



图例：安全厂商信创安全产品分布

目前国产化硬件性能参差不齐，操作系统环境及组件版本多种多样，给信创安全产品的兼容适配带来了很大挑战。下表简单列举了部分安全产品的信创适配挑战：

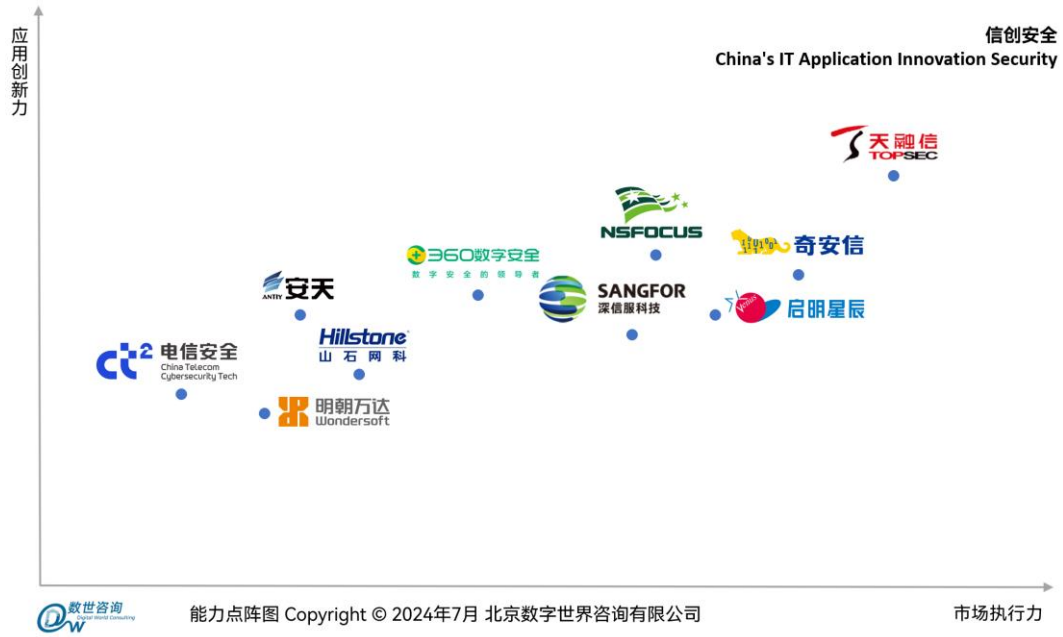
类别	代表产品	适配挑战
边界安全类	防火墙，上网行为管理、隔离网闸，抗DDoS，入侵检测与防御（IPS/IDS）、VPN等	厂商需在保持原有安全功能的前提下，适配国产化的CPU、芯片、存储部件等，同时对硬件电路进行定制化设计，并确保接口标准与数据传输稳定，软件采用国产化操作系统，功能上能够与现有信创环境兼容和协同工作。
终端安全类	终端杀毒、主机监控、终端检测与响应（EDR）等	信创终端类安全产品主要考虑芯片架构、整机、操作系统的适配。在不同的CPU指令集、不同操作系统环境下需要编译不同的软件版本。

安全管理类	态势感知，日志审计，保垒机等	态势感知和 SOC 类管理平台比其它安全软件的适配更加复杂，除了兼容适配以上提到的各种软硬件环境之外，还需要与底层的不同的数据库，以及数据库中间件等实现对接，同时还需要与大量第三方依赖组件进行适配。
云安全防护类	云安全资源池，云安全管理平台等	针对信创云多样化的架构和操作系统，安全防护需要适配云计算的不同底层架构，不同的虚拟化环境，需要支持“一云多芯”以适应多样化的信创生态环境。
数据安全类	数据库审计、数据防泄露、数据脱敏、文档加密等	数据安全类产品，需要适配国产化数据库的数据格式、能够对信创系统中的数据指令进行识别过滤。
国产密码类	数字证书、密码机、签名验签服务器等	产品首先采用国产化的硬件和操作系统，应用国产密码算法和技术，同时与下游大量软硬件产品的适配对接。

4 能力企业

4.1 信创安全骨干企业

国内二十余家信创安全厂商参与了本次调研，鉴于信创安全产品类型众多，不同安全厂商有不同的技术背景和发展路线，本报告只选择了十余家骨干企业进行点阵图的排名。分别是（按公司简称首字母排序）：360 数字安全、安天、电信安全、绿盟科技、明朝万达、奇安信、启明星辰、山石网科、深信服、天融信，按照横轴-市场执行力、竖轴-应用创新力，通过能力点阵图的方式展现如下：



图例：信创安全骨干企业点阵图

这些骨干企业走在国产化适配队伍的前列，大多在信息安全领域深耕多年，有着深厚的技术积累和丰富的项目经验。这些企业产

品的国产化率大多达到 70%以上，个别厂商超过 85%。企业信创研发能力的高低，除了与自身的技术积累有关之外，还与能够参与的信创项目的多寡有直接关系。显然，参与的项目越多，对信创生态环境的研究越深入，即能显著提升其产品的稳定性和解决方案的先进性。

部分企业的信创安全能力及主要信创产品介绍如下（按首字母序排列）：

企业	信创能力简介	信创主要领域或产品
360 数字安全	360 构建了以安全大脑为核心的新一代信创安全能力体系，同时 360 还整合漏洞挖掘、信创软件供应链安全、信创产品安全检测等方面能力，实现支撑信创软件全生命周期安全治理。	360 云脑、企业安全浏览器、高级持续威胁预警系统。
安天	安天是最早参与信创安全领域的厂商，基于 20 多年自主核心技术积累的反病毒引擎和网络安全产品，能力覆盖云、边、端以及工控和物联网等领域。已经适配龙芯、飞腾、申威、海光、鲲鹏等 cpu 厂商，也与统信、麒麟、方德等多个操作系统完成适配。	终端防御、终端检测与响应、云工作负载安全、网络检测与响应、应用安全防护、网络威胁分析（沙箱）。
电信安全	中国电信安全公司致力于打造具有行业特色的全栈信创安全产品，引领电信信创安全业务发展。目前全系安全产品开展信创适配改造，取得兼容互认证明 100+张，取得第三方检测报	信创态势感知平台，信创云安全产品（云主机安全，云 WAF、入侵检测）。

	告 10 份。	
绿盟科技	绿盟科技安全产品的核心部件（CPU、OS、网卡、内存）已完成与多种信创环境适配的工作，支持飞腾、海光、鲲鹏、兆芯 、申威 5 类 CPU，软件适配银河麒麟、统信两大国产化操作系统。在绿盟公司八大行业和全国各个区域均有多个成功部署的案例 。	漏洞扫描、入侵检测、抗 DDoS、WEB 应用防火墙、流量分析、下一代防火墙、数据库审计。
奇安信	奇安信深耕信创安全领域多年，目前已完成 70 类 200 余型号的信创安全产品研发。信创安全产品广泛服务于政企客户，其中政府、金融客户覆盖率居于市场前列。	终端防护、边界防护、身份鉴别、安全审计、运维安全管理、流量控制、信息泄露防护。
山石网科	基于国产芯片和国产操作系统，山石网科发挥自身 10 余年硬件设计与软件研发的技术优势，陆续推出多个系列信创产品，包括国内第一款吞吐超百 G 的国产化高端数据中心防火墙等多个品类信创安全产品。	防火墙、入侵防御和 web 应用防火墙、应用交付、安全审计和运维安全网关、日志审计平台、数据库审计、漏洞扫描。
天融信	天融信多年来深耕信创安全领域技术研究，重点推动全栈国产化能力建设，2010 年启动国产 CPU 芯片应用研究。通过与国产 CPU、操作系统、数据库、浏览器、中间件等生态上下游企业的紧密合作，天融信将基础软硬件、国密算法、可信技术等进行深度融合，截至目前共发布 69 类 260 余款信创安全产品，累计获取各	防火墙、VPN、WAF、IPS、IDS、超融合、网闸、漏扫、EDR、堡垒机、日志审计、态势感知、数据防泄露、数据库审计、云桌面、工控防

	类兼容性互认证书 2300+项。目前产品和方案已在党政、金融、能源、交通等近 30 个行业实现规模化应用。	火墙、负载均衡、安全资源池。

4.2 信创安全细分领域访谈企业

尽管信创安全产业正处于快速发展的关键时期，然而由于不是所有行业的信创策略能够同步推进，加之一些领域在信息安全产品适配时面临众多困难，信创安全细分领域仅有少数安全企业针对国产化推进做好了准备。

以下是参与本次调研与访谈的部分细分领域安全企业。这些企业在信创安全领域，都较早的投入信创安全产品适配和研发工作，而且产品在不同行业应用落地。

企业	细分领域	信创能力简介	信创产品
安普诺(悬镜安全)	数字供应链安全/DevSecOps	提供基于代码疫苗技术的信创数字供应链安全治理与运营解决方案。其创新性代码疫苗技术填补了国内在数字供应链安全领域的技术空白并解决了关键技术卡脖子问题。	开源威胁管控、白盒/灰盒安全测试、代码审计、供应链安全情报、渗透测试平台。
方向标	邮件安全	北京方向标公司从 2019 年开始进行自主品牌发展建设和信创化邮件安全产品	邮件安全网关、邮件归

		与运营服务之路。得益于国产化替代和信创项目的经验积累，方向标公司显示了极为充分的产品实力，将识别率、误判率分别提高到一个全新的高度。	档、邮件防泄密系统。
海云安	代码安全	海云安产品完全自主研发，适配企业信创环境要求，在系统自身信创性、信创环境兼容性、信创检测能力这三方面表现突出。	源代码检测分析管理系统、开源组件安全检测系统。
华顺信安	网络资产测绘	基于网络空间测绘技术，以信创软硬件资产为主要标的。致力于解决企业在信创环境下所面临的安全挑战，通过对企业信创资产进行测绘，识别潜在的安全风险，并提供针对性的防护策略。	网络资产测绘及风险分析系统。
联成科技	安全运营	采用国产服务器、操作系统、网络设备及安全软件产品，为用户搭建安全可靠、国产可控的基础环境和基础软件平台，支撑业务系统平稳运行。	安全运维管理平台。
明朝万达	数据安全	明朝万达的主要产品是数据防泄漏和数据安全治理，是较早实施信创数据安全产品的适配，数据安全方面入选信创目录比较全而且比较早的厂商之一。	终端 DLP 、网络 DLP 、数据库脱敏系统、日志审计系统、数据管理平台。

软极网络	仿真模拟	致力于与国产化运行环境深度适配，模拟仿真主流软硬件系统环境，提供信创测试环境和平台。	信创靶场平台。
世安智慧	安全审计	基于国产芯片和国产操作系统，发布了基于兆芯、龙芯等 CPU，统信、银河麒麟等操作系统的国产化系列产品。	网络准入控制系统、安全运维管理平台。
网藤科技	工控安全	与国内主流的芯片、操作系统及各类应用厂商完成兼容性认证，提供电力、石油化工、制造、矿山、轨交等行业所需需的国产化工控安全产品。	隔离网闸、工控主机安全、工业防火墙、日志审计分析系统。
云弈科技	云安全	致力于国家网络空间安全监测、防护和治理，以信创安全为核心理念，为客户提供综合性安全解决方案。	主机安全、网站云防御平台、运维管理与审计平台、资产脆弱性扫描与管理。
丈八网安	测试平台	信创应用模拟与测试。	信创网络靶场、信创安全测试评估系统。

5 市场洞察

信创安全建设需要体系化的设计和真正满足业务安全需求

当前，信创安全主要还是依靠政策驱动，市场驱动的力量相对较弱。对安全厂商来说，产品适配也更多依赖于项目驱动，大部分安全厂商缺乏系统化的信创安全适配规划。对用户来说，由于信创安全方案的渗透率较低，安全产品应用多局限于单点防护，用户对如何建设完整的安全运营体系没有清晰的思路。

信创软硬件环境及生态的不确定性，使得信创安全市场竞争和技术发展方向的不确定性增加

信创安全生态环境的稳定性受到整体信创生态环境的影响，特别是在市场竞争和技术发展方向的不确定性增加。市场竞争方面，随着更多安全厂商进入信创市场，产品和方案的竞争愈发激烈，可能导致一些产品或方案逐渐退出市场。技术层面，关键技术的成熟度尚未能完全替代非国产化技术，例如芯片性能、中间件功能、底层系统的稳定性等，这也给信创安全产品的国产化适配带来极大的不确定性。在供应链层面，信创软件供应链仍然非常脆弱，大量开源框架、开源代码的引入，也会带来非常多的未知挑战。

那些尽早开始信创适配，投入资源积极进行技术攻关的厂商，已在信息安全市场中获得先机

信创安全产品的兼容适配工作需要克服多样化的技术挑战，包括但不限于不同芯片、操作系统版本以及诸多依赖组件。这不仅要求建立相应的开发与测试环境，还需在实际信创环境中进行反复的运行测试，产品通常需经过多轮研发和功能验证，才能达到稳定成熟交付。那些尽早开始信创适配，投入资源积极进行技术攻关的厂商，已在信息安全市场中获得先机。

信创安全不仅仅是“国产替代”，安全厂商需要与信创上下游供应商共建信创生态

信创安全的发展依赖于信创产业的支持，但是目前发展中的信创基础架构还存在不少安全漏洞和安全风险。安全企业应当利用其在网络安全领域的专业知识和技术优势，协助完成信创软硬件基础设施的漏洞发现和风险管理的工作，与上下游产业伙伴紧密合作，共建信创生态。

6 未来展望

随着党政、金融、电信几大行业信创排头兵完成试点应用，信创产业将在各行业全面铺开建设，信创安全市场也必将迎来爆发式增长，这个发展态势大家有目共睹。未来几年信创安全领域发展趋势有以下五“+”：

一、信创安全产品性能提升 + 功能同步完善

目前国产 CPU 性能与国际厂商相比仍存在差距，导致信创安全产品的性能难以达到非信创产品的水平。未来随着 CPU 厂商加速迭代，推出更高性能的 CPU，可望不断提升信创安全产品的处理性能。产品性能提升的同时也会促进功能的完善，比如对应用层协议的解析、应用威胁检测、数据加解密等等。

二、信创安全多场景适配 + 体系化解决方案

信创安全产品的发展呈现出多场景适配和体系化建设的趋势。一方面，针对不同行业的应用场景，例如工控、大数据、物联网等，信创安全产品需要提供定制化的安全方案，满足不同信息基础设施的需求。另一方面，在“三同步”规划及体系化建设原则的指导下，信创安全产品从单点的安全防护向体系化安全建设发展。笔者调研了解到，几大骨干信创安全厂商正在积极推动全系列信创安全产品适配，并且在打造综合性安全解决方案上下功夫。

三、信创安全原生融合 + 生态环境共建

信创安全原生融合一方面是指是在研发信创安全新产品时，在立项阶段就会考虑产品信创化适配。另一方面是指加强和信创厂商的生态合作，将安全能力直接赋能给信创生态厂商，通过供应链上游赋能提升信创产品原生安全能力。安全厂商与信创企业之间的合作共建将推动信创生态的快速裂变，促进安全技术的应用和推广。

四、信创安全云化 + 服务化交付

为适应随着越来越多的业务集中化运营和管理的需要，信创云的建设是未来的一大趋势之一，信创云安全也是首先必须要考虑的基础问题。云计算的建设模式下，安全也会更多通过即服务的模式向企业交付。

五、智能化演化加速 + 应用创新

随着人工智能技术的快速发展以及近期大模型技术与信息安全的融合，信创安全产品、信创安全工具的智能化水平正在加速演化。信创安全站在传统信息安全巨人的肩膀上，未来也必能持续在技术应用创新方向投入和转化，信创安全产业大发展未来可期！

附件：省税务局国产化运维建设项目

本案例由 天融信 提供

项目背景

某省税务局为满足税务专网运维与信息化建设需求，计划在数据中心搭建云平台，部署虚拟化软件，虚拟化麒麟操作系统，满足160 名第三方运维人员日常运维，同时为省局机关各类审计、总局督导检查等工作组预留 50 个虚拟化计算机资源及终端，并结合省局税务的业务系统需求，部署超融合云服务平台，为某业务快速上线及部署测试提供稳定的基础环境。

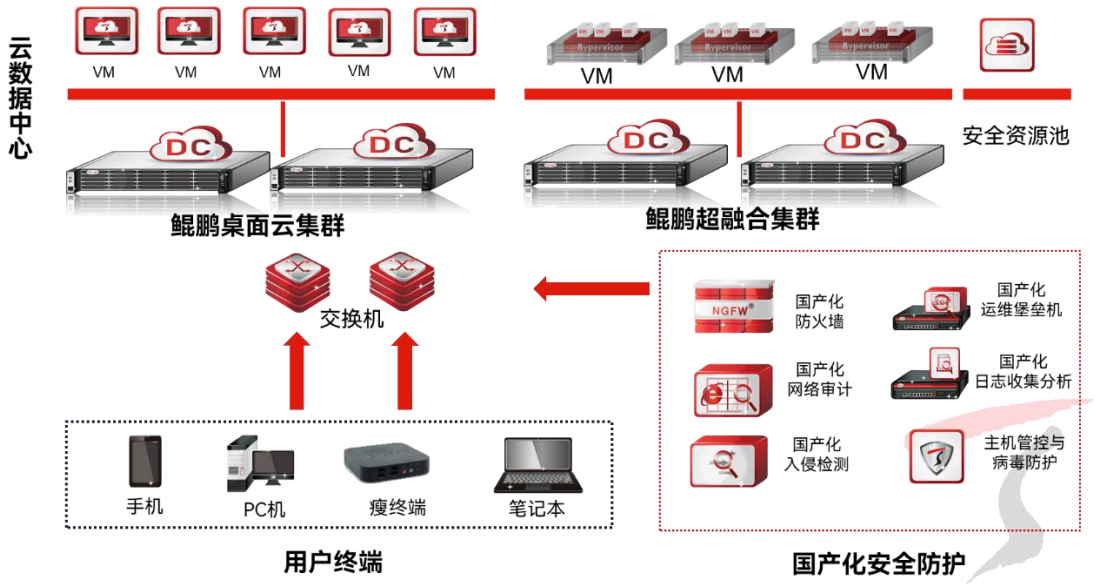
客户痛点

税务专网全省联通，目前专网内设备、软件、应用工作量巨大，某省税务局配置专门的运维团队开展运维工作。但运维人员大多为外包，难以依靠制度全部落地，面临数据安全合规要求落地难、日常审计规范性不足等问题，故采取统一终端建设模式，引入桌面云建设满足数据安全与访问审计要求。此次云桌面建设需充分考虑某业务系统快速上线及测试的环境支撑诉求，确保数据不落地，同时还需具有访问审计功能，可控制数据访问入口及出口，防范数据拷出、违规外联等事件发生。

解决方案

天融信采用桌面虚拟化和服务器虚拟化解决方案替代传统 PC 机

的办公模式，在数据中心部署高性能桌面云服务器集群、超融合集群，依托统一管理平台实现对硬件资源、虚拟资源、存储服务、云终端的一体化监控、运维和升级。方案采用全冗余设计架构，提供虚拟机 HA（高可用）、DRS（动态资源调度）、DPM（动态电源管理）等功能，帮助运维人员实现了智能极简、无忧运维，确保业务的安全稳定运行。通过方案的实施，大幅降低管理成本并提升设备利用率，打造智能绿色低碳办公场景。



通过天融信桌面云系统的产品关键组件，以软件定义的形式构建，提供统一的云端管理，云端计算服务，有效简化运维管理，降低信息泄露风险，提升系统安全，并实现终端零数据，满足省税务局信息化发展需求。天融信桌面云系统支持外设管理，提供安全运维管理手段；支持应用管理，限制办公电脑无关软件；支持上网管理，限制用户上网；支持流量管理，管控用户上网流量；支持云桌

面热迁移，桌面灵活扩展，自动将资源负载均衡等功能。

通过天融信超融合管理系统实现计算虚拟化、网络虚拟化、存储虚拟化和安全虚拟化，将各国产化服务器上的 CPU、内存、硬盘、网络进行抽象、池化，对外提供自动化的调配，通过全虚拟化的方式构建 IT 架构资源池。所有的模块资源均可以按需部署，灵活调度，动态扩展，且全部是由统一的管理界面呈现，提供简单便捷的运维体验操作。

通过部署虚拟化下一代防火墙、虚拟化 Web 应用防火墙、虚拟化基线核查等安全组件，为云中心的主机、网络、应用、数据等资产提供全方位的安全保障。通过部署国产化的防火墙、运维堡垒机、网络审计、入侵检测、日志收集分析和适配国产化操作系统的主机管控与病毒防护系统，从边界安全、运维安全、安全审计、安全检测、终端管控、防病毒等多方位多角度实现安全防护，提升了省税务局国产化运维项目安全保障能力和自主可控能力。

客户价值

采用国产化鲲鹏服务器，自研可控的桌面云和超融合软件，并根据等级保护要求部署国产化网络安全设备，全面提升自主可控安全能力。

云桌面可确保数据不落地，敏感数据集中存储，保障数据安全；超融合平台能够为客户提供稳定的国产支撑平台环境，保障业务系

统按期上线交付测试。全面管控提升内网安全，访问审计功能可严格控制数据访问出入，防止数据违规拷贝、违规外联等事件发生。

统一终端管理全面提升管理运维效率，全面确保桌面连续使用。

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