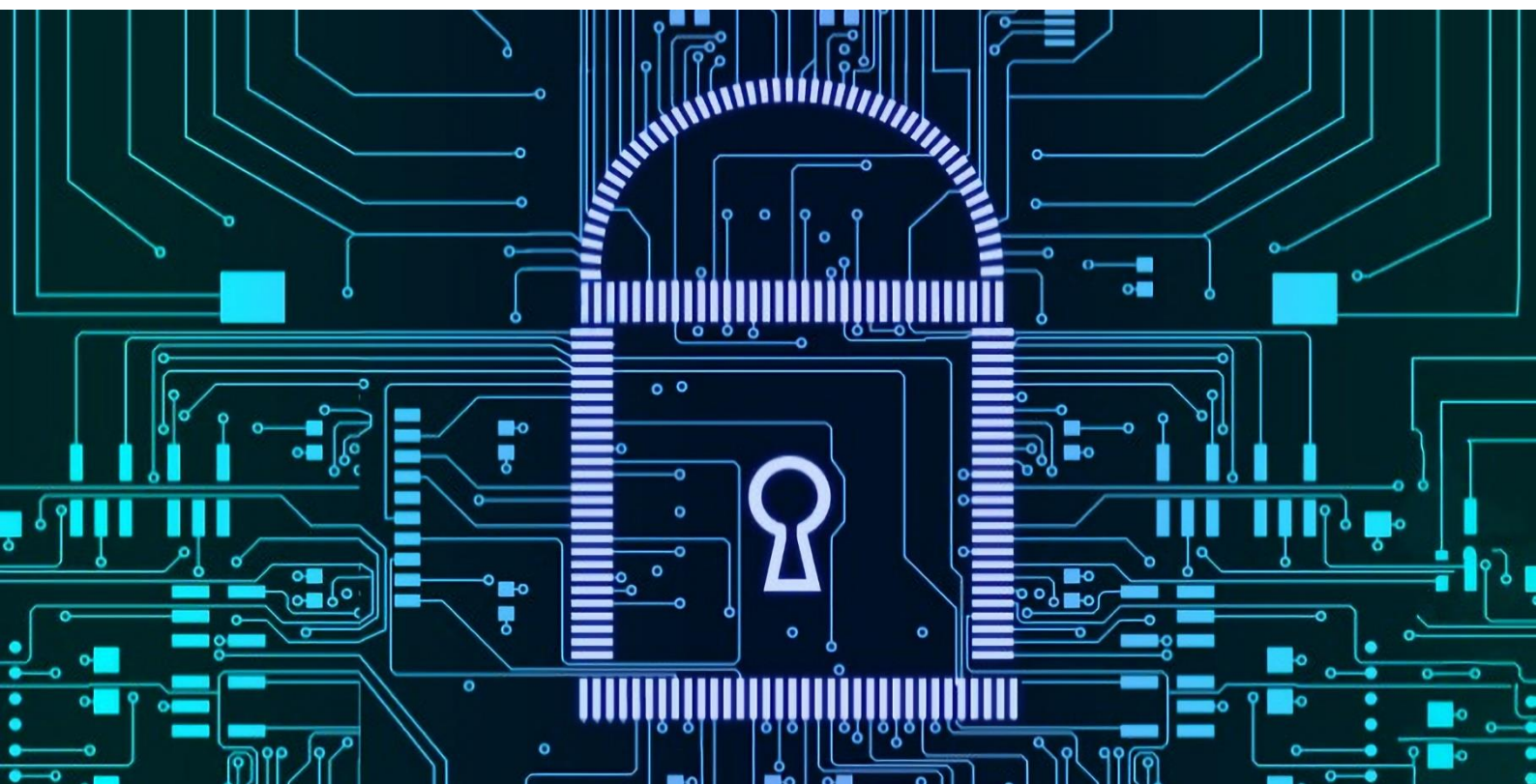
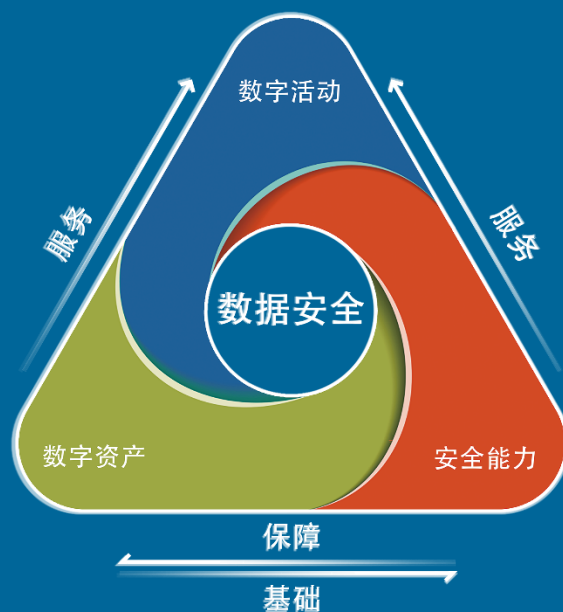


信创安全市场指南



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、网安企业等合作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

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

1 前言	5
2 关键发现	6
3 市场概况	7
3.1 概述	7
3.2 定义与范围	8
3.3 市场规模	9
3.4 行业分布	10
3.5 信创安全产品	11
4 能力企业	15
4.1 信创安全骨干企业	15
4.2 信创安全细分领域访谈企业	18
5 市场洞察	21
6 未来展望	23
附件：省税务局国产化运维建设项目	25

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](mailto:chenfaming@dwcon.cn)
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。

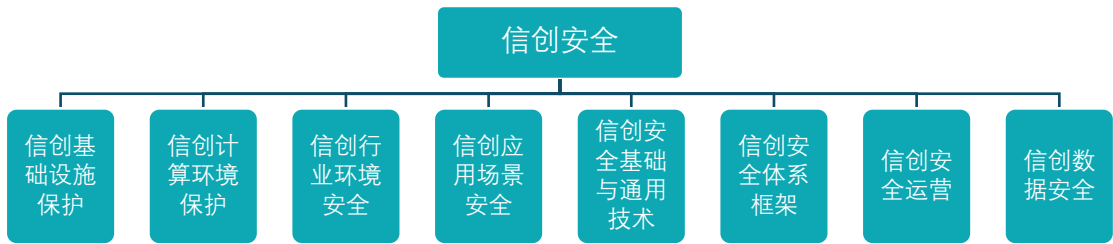
3.2 定义与范围

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

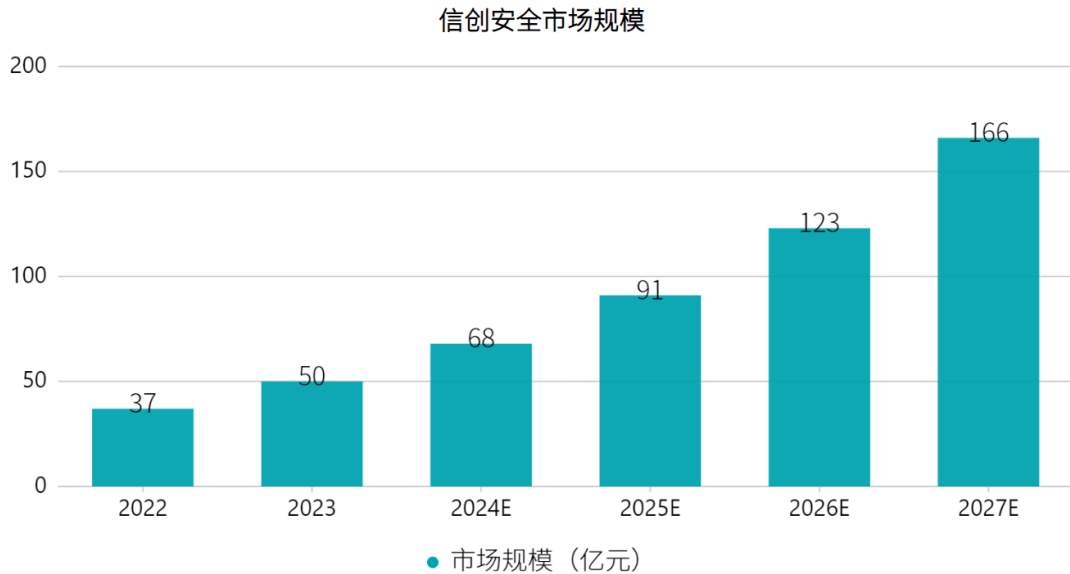
3.3 市场规模

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。



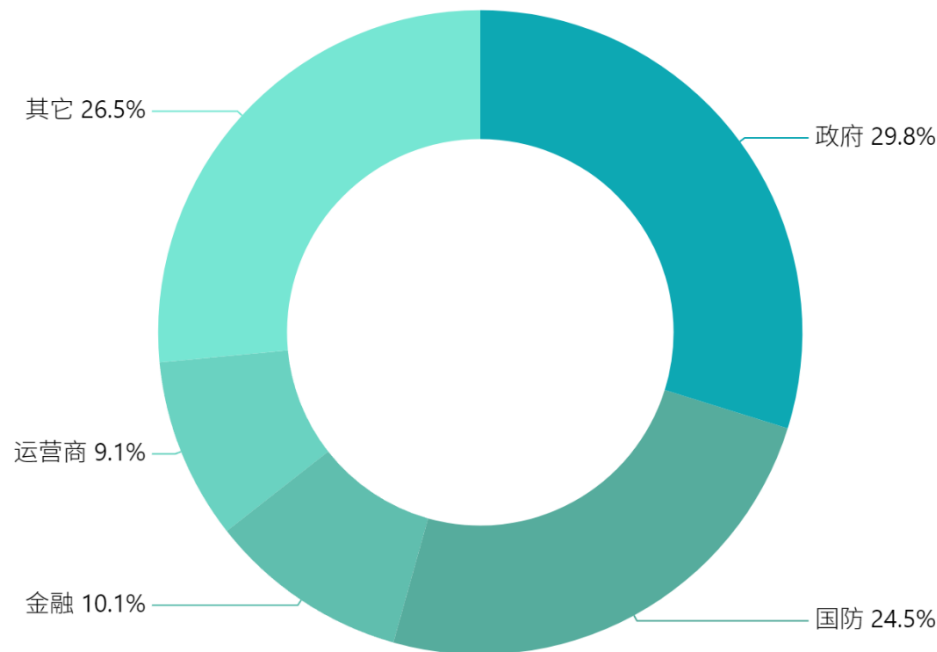
图例：信创安全市场规模

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%）。

信创安全行业分布



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 and 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。

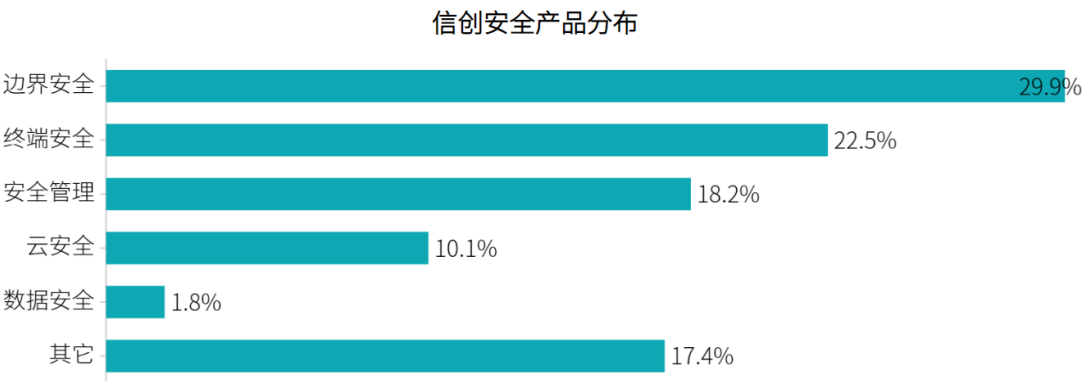
工业软件和工控系统的国产化仅有部分厂商尽早进行了适配工作。信创工控安全产品主要有：工控网闸、工业防火墙、边界审计系统、数据交换审查审批系统等。

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：

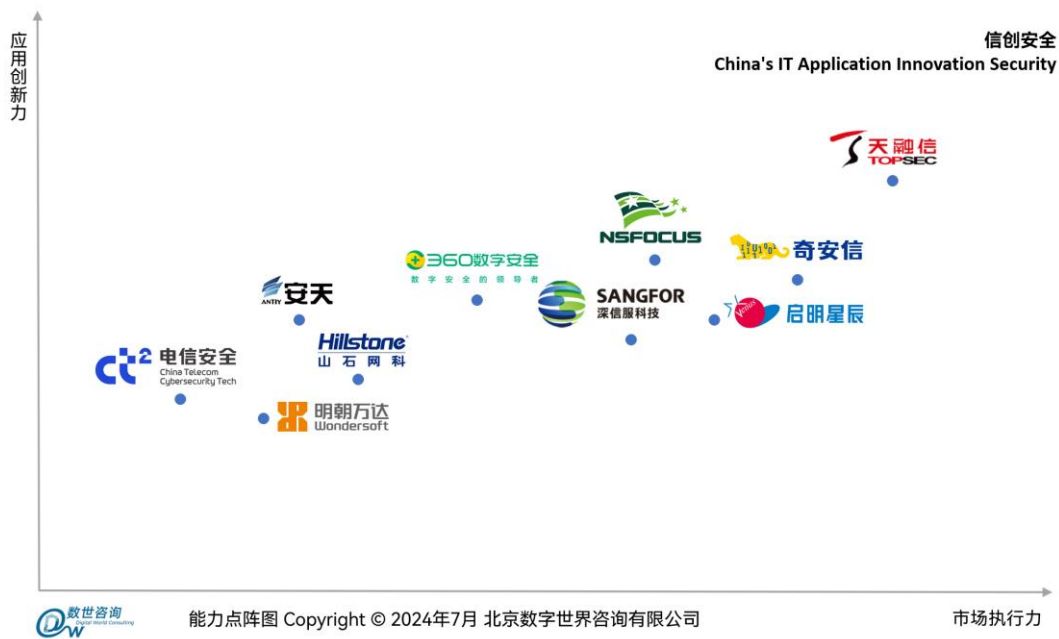
类别	代表产品	适配挑战
边界安全类	防火墙，上网行为管理、隔离网闸，抗DDoS，入侵检测与防御（IPS/IDS）、VPN等	厂商需在保持原有安全功能的前提下，适配国产化的CPU、芯片、存储部件等，同时对硬件电路进行定制化设计，并确保接口标准与数据传输稳定，软件采用国产化操作系统，功能上能够与现有信创环境兼容和协同工作。
终端安全类	终端杀毒、主机监控、终端检测与响应（EDR）等	信创终端类安全产品主要考虑芯片架构、整机、操作系统的适配。在不同的CPU指令集、不同操作系统环境下需要编译不同的软件版本。

安全管理类	态势感知，日志审计，堡垒机等	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

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：<https://d.book118.com/576233213223010204>