# 安恒信息（688023.SH）

## 新型安全龙头，引领安全能力服务化趋势

**安恒信息：面向“新技术”、“新场景”的网络安全信息产品和服务商。**安恒信息成立于 2007 年，业务覆盖应用安全、大数据安全、云安全、物联网安全、工业控制安全及工业互联网安全等多个领域。公司围绕云计算、大数据以及物联网等新一代信息技术，形成了以“新场景”及“新服务”为方向的专业安全平台产品和服务体系。董事长兼实控人持股 27.02%，阿里为第二大股东，持有公司 5%以上的股东均出具《不谋求发行人控制权的承诺函》，中长期公司股权结构预计保持稳定。

**安全市场需求强劲，产业向服务主导转型。1）国内安全市场保持高速增长，**渗透空间巨大 IDC 预测，2019 年中国安全解决方案总体支出将达到 69.5 亿美元(不含 IoT 安全)，2018 年~2022 年预测期内的年复合增长率为 25.6%，到 2022 年，市场规模将增长至 137.7 亿美元。中国安全投入/IT 投入占比（1.84%）与全球（3.74%）差距较大，网络安全市场仍有很大渗透空间。**2）政策是安全行业主要驱动力，等保 2.0 利好安全服务产品。**网络安全已上升到国家战略，政府、通信、金融是安全主要下游，政策是行业主要驱动力。等保 2.0 相对 1.0 扩宽了监管范围与监管内容，促进了态势感知类产品和主动防御市场等安全服务类产品的快速增长。**3）安全产业向服务主导转型，云安全服务将成为细分潜力最大的安全市场。**随着中国云安全服务生态逐渐形成。云安全服务将成为细分潜力最大的安全市场。根据赛迪统计，2018 年，中国云安全服务市场规模达到 37.8 亿元，同比 2017 年增长 44.8%，预计到 2021 年中国云安全服务市场规模将达到 115.7 亿元，未来三年年均增长率为 45.2%，行业正处爆发式增长趋势。**4）5G 多样化场景与技术革新带来安全增量。**

**“战略+技术”成就产品高增长，引领安全服务演绎新模式 1）态势感知、云安全、AiLPHA 大数据持续推动平台高速增长：**公司是态势感知市场的领导者，是公安和网信行业态势感知的主要建设者和推动者。根据安全牛，预计 2020 年态势感知整体市场规模将超过 50 亿元，CAGR 达 35.72%；AiLPHA 大数据智能安全平台集成超大规模存查、大数据实时智能分析等安全模块，为客户提供全局态势感知，打造智能安全运营新模式；同时公司是公有云、私有云、多云混云安全方案全面部署的第三方厂商。**2）安全服务：一切产品皆资源，一切资源皆服务：**网络安全服务正在走向第五代服务模式，数据驱动即服务，强依赖自主运营的智能服务，就是安全能力的服务化。

**给予“买入”评级。**预计公司 2020-2022 年营业收入分别为 14.37/21.46/31.88 亿元，增速分别为 52.26%、49.30%、48.57%；归母净利润分别为 1.69/3.14/6.19 亿元，增速分别为 83.54%、85.59%、97.02%，对标美国 CrowdStrike，给予“买入”评级。

**风险提示：**行业竞争加剧；公司安全服务与平台增速推进不及预期；关键假设可能存在误差的风险。

| 财务指标 | 2018A | 2019A | 2020E | 2021E | 2022E |
|---|---|---|---|---|---|
| 营业收入（百万元） | 627 | 944 | 1,437 | 2,146 | 3,188 |
| 增长率 yoy（%） | 45.6 | 50.7 | 52.3 | 49.3 | 48.6 |
| 归母净利润（百万元） | 77 | 92 | 169 | 314 | 619 |
| 增长率 yoy（%） | 47.5 | 20.0 | 83.5 | 85.6 | 97.0 |
| EPS 最新摊薄（元/股） | 1.04 | 1.24 | 2.29 | 4.24 | 8.36 |
| 净资产收益率（%） | 14.9 | 5.9 | 9.8 | 15.4 | 23.3 |
| P/E（倍） | 205.7 | 171.5 | 93.4 | 50.3 | 25.6 |
| P/B（倍） | 31.2 | 10.2 | 9.2 | 7.8 | 6.1 |

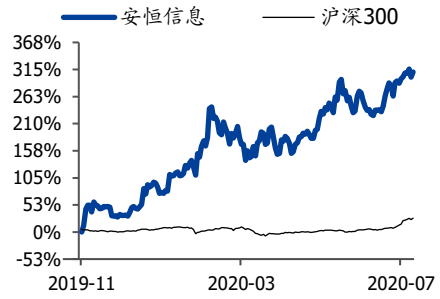
*资料来源：贝格数据，国盛证券研究所*

**买入（首次）**

**股票信息**

| | |
|---|---|
| 行业 | 计算机应用 |
| 最新收盘价 | 323.79 |
| 总市值(百万元) | 23,984.44 |
| 总股本(百万股) | 74.07 |
| 其中自由流通股(%) | 21.87 |
| 30 日日均成交量(百万股) | 0.28 |

**股价走势**




**作者**

**分析师 刘高畅**
执业证书编号：S0680518090001
邮箱：liugaochang@gszq.com
**分析师 安鹏**
执业证书编号：S0680519030002
邮箱：anpeng@gszq.com

## 财务报表和主要财务比率

资产负债表（百万元）

| 会计年度 | 2018A | 2019A | 2020E | 2021E | 2022E |
|---|---|---|---|---|---|
| **流动资产** | 664 | 1853 | 2114 | 2640 | 3496 |
| 现金 | 398 | 1483 | 1471 | 1797 | 2183 |
| 应收票据及应收账款 | 170 | 201 | 364 | 480 | 773 |
| 其他应收款 | 40 | 41 | 82 | 102 | 171 |
| 预付账款 | 3 | 5 | 8 | 11 | 17 |
| 存货 | 49 | 116 | 183 | 243 | 345 |
| 其他流动资产 | 5 | 7 | 7 | 7 | 7 |
| **非流动资产** | 227 | 319 | 329 | 361 | 432 |
| 长期投资 | 21 | 20 | 12 | 2 | -12 |
| 固定资产 | 33 | 281 | 296 | 337 | 423 |
| 无形资产 | 8 | 7 | 7 | 7 | 5 |
| 其他非流动资产 | 165 | 11 | 14 | 15 | 16 |
| **资产总计** | 892 | 2172 | 2443 | 3001 | 3928 |
| **流动负债** | 299 | 499 | 622 | 881 | 1199 |
| 短期借款 | 0 | 0 | 0 | 0 | 0 |
| 应付票据及应付账款 | 100 | 156 | 228 | 358 | 530 |
| 其他流动负债 | 199 | 343 | 394 | 523 | 669 |
| **非流动负债** | 86 | 123 | 101 | 86 | 77 |
| 长期借款 | 81 | 107 | 86 | 70 | 62 |
| 其他非流动负债 | 5 | 16 | 16 | 16 | 16 |
| **负债合计** | 385 | 622 | 724 | 967 | 1276 |
| 少数股东权益 | 0 | 0 | -0 | -0 | -1 |
| 股本 | 56 | 74 | 74 | 74 | 74 |
| 资本公积 | 309 | 1242 | 1242 | 1242 | 1242 |
| 留存收益 | 142 | 234 | 404 | 718 | 1336 |
| 归属母公司股东权益 | 507 | 1550 | 1720 | 2034 | 2653 |
| **负债和股东权益** | 892 | 2172 | 2443 | 3001 | 3928 |

现金流量表（百万元）

| 会计年度 | 2018A | 2019A | 2020E | 2021E | 2022E |
|---|---|---|---|---|---|
| **经营活动现金流** | 96 | 217 | 84 | 467 | 607 |
| 净利润 | 76 | 92 | 169 | 314 | 619 |
| 折旧摊销 | 13 | 24 | 44 | 55 | 72 |
| 财务费用 | -2 | -3 | 12 | 32 | 59 |
| 投资损失 | 1 | 2 | 7 | 9 | 13 |
| 营运资金变动 | 1 | 88 | -148 | 57 | -156 |
| 其他经营现金流 | 8 | 13 | 0 | 0 | 0 |
| **投资活动现金流** | 9 | -119 | -61 | -96 | -156 |
| 资本支出 | 95 | 127 | 18 | 42 | 85 |
| 长期投资 | 102 | -0 | 8 | 17 | 14 |
| 其他投资现金流 | 206 | 8 | -35 | -37 | -57 |
| **筹资活动现金流** | 74 | 988 | -34 | -46 | -65 |
| 短期借款 | 0 | 0 | 0 | 0 | 0 |
| 长期借款 | 71 | 26 | -21 | -15 | -9 |
| 普通股增加 | 0 | 19 | 0 | 0 | 0 |
| 资本公积增加 | -2 | 933 | 0 | 0 | 0 |
| 其他筹资现金流 | 5 | 11 | -13 | -31 | -56 |
| **现金净增加额** | 179 | 1086 | -12 | 325 | 386 |

利润表（百万元）

| 会计年度 | 2018A | 2019A | 2020E | 2021E | 2022E |
|---|---|---|---|---|---|
| **营业收入** | 627 | 944 | 1437 | 2146 | 3188 |
| 营业成本 | 185 | 288 | 433 | 659 | 999 |
| 营业税金及附加 | 8 | 12 | 17 | 23 | 29 |
| 营业费用 | 206 | 316 | 427 | 555 | 693 |
| 管理费用 | 59 | 85 | 109 | 136 | 163 |
| 研发费用 | 152 | 205 | 297 | 416 | 562 |
| 财务费用 | -2 | -3 | 12 | 32 | 59 |
| 资产减值损失 | -8 | -3 | 14 | 43 | 64 |
| 其他收益 | 65 | 59 | 74 | 94 | 118 |
| 公允价值变动收益 | 0 | 0 | 0 | 0 | 0 |
| 投资净收益 | -1 | -2 | -7 | -9 | -13 |
| 资产处置收益 | 0 | 0 | 0 | 0 | 0 |
| **营业利润** | 74 | 92 | 197 | 367 | 725 |
| 营业外收入 | 1 | 0 | 3 | 4 | 4 |
| 营业外支出 | 0 | 1 | 1 | 1 | 2 |
| **利润总额** | 75 | 91 | 199 | 369 | 728 |
| 所得税 | -1 | -1 | 30 | 55 | 109 |
| **净利润** | 76 | 92 | 169 | 314 | 619 |
| 少数股东损益 | -1 | -0 | -0 | -0 | -0 |
| **归属母公司净利润** | 77 | 92 | 169 | 314 | 619 |
| EBITDA | 81 | 78 | 202 | 378 | 742 |
| EPS（元/股） | 1.04 | 1.24 | 2.29 | 4.24 | 8.36 |

主要财务比率

| 会计年度 | 2018A | 2019A | 2020E | 2021E | 2022E |
|---|---|---|---|---|---|
| **成长能力** | | | | | |
| 营业收入（%） | 45.6 | 50.7 | 52.3 | 49.3 | 48.6 |
| 营业利润（%） | 29.9 | 24.5 | 113.8 | 86.2 | 97.7 |
| 归属母公司净利润（%） | 47.5 | 20.0 | 83.5 | 85.6 | 97.0 |
| **获利能力** | | | | | |
| 毛利率（%） | 70.5 | 69.5 | 69.9 | 69.3 | 68.7 |
| 净利率（%） | 12.3 | 9.8 | 11.8 | 14.6 | 19.4 |
| ROE（%） | 14.9 | 5.9 | 9.8 | 15.4 | 23.3 |
| ROIC（%） | 11.6 | 3.2 | 7.3 | 12.8 | 20.7 |
| **偿债能力** | | | | | |
| 资产负债率（%） | 43.1 | 28.6 | 29.6 | 32.2 | 32.5 |
| 净负债比率（%） | -60.4 | -86.2 | -78.4 | -83.0 | -78.4 |
| 流动比率 | 2.2 | 3.7 | 3.4 | 3.0 | 2.9 |
| 速动比率 | 2.0 | 3.5 | 3.1 | 2.7 | 2.6 |
| **营运能力** | | | | | |
| 总资产周转率 | 0.8 | 0.6 | 0.6 | 0.8 | 0.9 |
| 应收账款周转率 | 4.5 | 5.1 | 5.1 | 5.1 | 5.1 |
| 应付账款周转率 | 2.3 | 2.2 | 2.2 | 2.2 | 2.2 |
| **每股指标（元）** | | | | | |
| 每股收益（最新摊薄） | 1.04 | 1.24 | 2.29 | 4.24 | 8.36 |
| 每股经营现金流（最新摊薄） | 1.30 | 2.92 | 1.13 | 6.31 | 8.19 |
| 每股净资产（最新摊薄） | 6.84 | 20.93 | 23.21 | 27.46 | 35.81 |
| **估值比率** | | | | | |
| P/E | 205.7 | 171.5 | 93.4 | 50.3 | 25.6 |
| P/B | 31.2 | 10.2 | 9.2 | 7.8 | 6.0 |
| EV/EBITDA | 190.5 | 185.5 | 71.6 | 37.4 | 18.5 |

*资料来源：贝格数据，国盛证券研究所*

## 内容目录

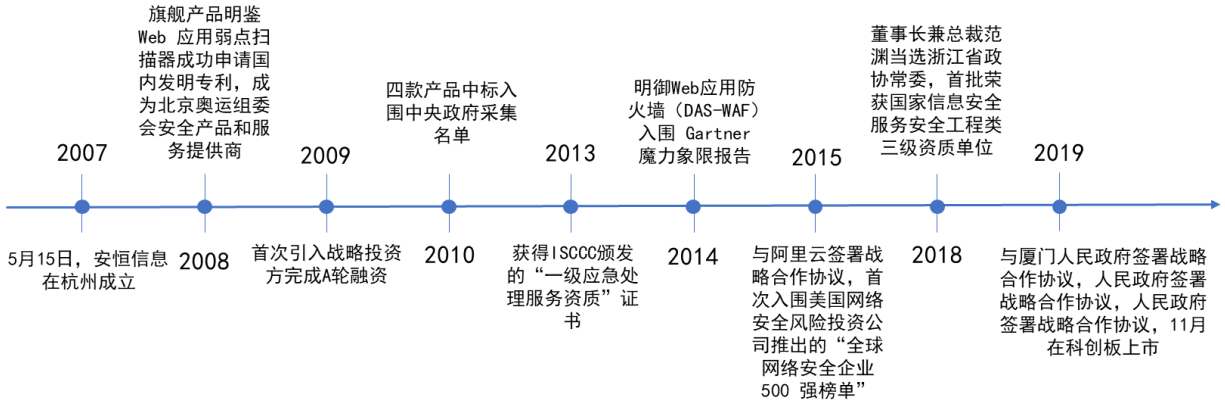


## 图表目录

## 安恒信息：面向“新技术”、“新场景”的网络安全信息产品和服务商

**安恒信息：国内领先的网络安全信息产品和服务商。**安恒信息成立于 2007 年，始终专注于网络信息安全，目前已成为国内领先的新时代网络安全信息产品和服务商。公司业务覆盖应用安全、大数据安全、云安全、物联网安全、工业控制安全及工业互联网安全等多个领域，成为了北京奥运会、上海世博会、深圳大运会、十八大人大代表大会、APEC 会议等多个重大活动及会议的网络安全技术提供商。自 2015 年入选全球网络安全创新 500 强之后，历年均被美国著名网络安全风险投资公司（Cybersecurity Ventures）评选为全球网络安全创新 500 强，并于 2014、2018 年两度进入 Gartner Web 应用防火墙魔力象限。

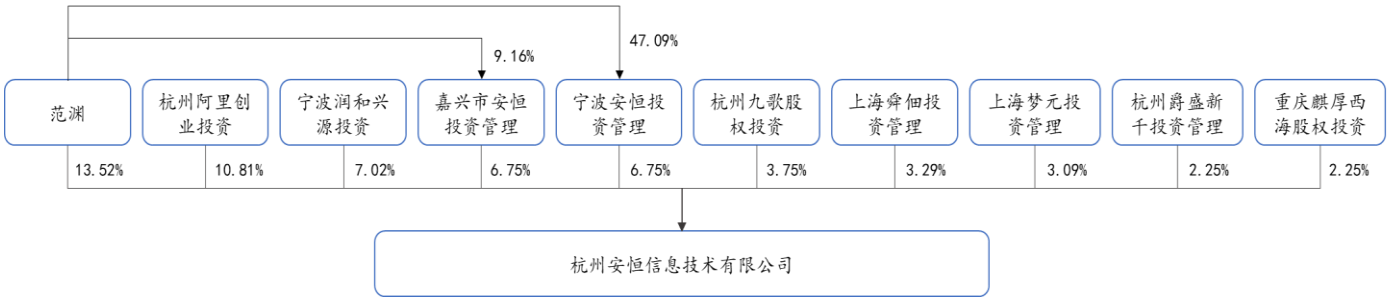
*图表 1：公司发展历程*




*资料来源：公司官网，国盛证券研究所*

**董事长兼实控人持股 27.02%，阿里为第二大股东。**公司第一大股东及实际控制人范渊先生直接持股 13.52%，通过嘉兴安恒、宁波安恒分别间接持股 0.62%、3.18%的股份。嘉兴安恒、宁波安恒为范渊先生的一致行动人，范渊先生共控制安恒信息 27.02%的表决权。公司第二大股东为阿里创投，占 10.81%股权。实际控制人范渊先生从事网络安全行业多年，是第一个登上全球顶级信息安全大会 BLACKHAT（黑帽子）大会进行演讲的中国人，有着丰富的技术开发和产品服务经验。持有公司 5%以上的股东均出具《不谋求发行人控制权的承诺函》，中长期公司股权结构预计保持稳定。

*图表 2：公司股权结构*




*资料来源：Wind，国盛证券研究所*

**依托资深优质的网络安全产品、情报威胁系统以及持续研发，公司围绕云计算、大数据以及物联网等新一代信息技术，形成了以“新场景”及“新服务”为方向的专业安全平**

**台产品和服务体系。**“新场景”是公司在新的监管要求、新的信息技术下提出的具有针对性的综合信息安全解决方案，如网络安全态势感知预警平台、AiLPHA 大数据智能安全平台等。在信息化快速发展的时代，做到网络安全全面感知、检测预警、通报处置和监管追溯的闭环，提升网络安全监管和决策能力。“新服务”寓意着公司从提供专业产品转变为提供专业服务，为顾客提供从安全规划、安全设计、安全建设到安全运营的一站式服务。

*图表 3：以“新场景”及“新服务”为方向的专业安全平台产品和服务体系*


*资料来源：公司招股说明书，国盛证券研究所*

**公司核心基础产品持续多年市场份额位居行业前列，前瞻性和影响力获得国内外权威机构认可。**根据赛迪顾问，公司的数据库审计和风险控制、运维审计与风险控制、Web 应用弱点扫描、态势感知平台等多个产品市场占比名列前茅，用户认可度高。此外，公司的核心产品 Web 应用防火墙自发布后，两次入围 Gartner 魔力象限推荐品牌；情报威胁产品入围 IDC 中国威胁情报安全服务 MarketScape；网络安全态势感知预警平台在 2018 年安全牛发布的市场研究报告中，在态势感知象限排名第一。

*图表 4：公司核心产品持续多年市场份额位居行业前列*

| 产品名称 | 市场份额及排名 | 数据来源 |
|---|---|---|
| Web 应用防火墙 | 2017 年度市场占比 16.7%，排名第 2 | Frost&Sullivan |
| 数据库审计与风险控制系统 | 2017 年度市场占比 7.2%，排名第 2<br>2016 年度市场占比 4.4%，排名第 4 | 赛迪顾问 |
| 运维审计与风险控制系统 | 2016 年度市场占比 14.5%，排名第 3 | 赛迪顾问 |
| Web 应用弱点扫描、远程安全评估系统 | 2017 年度市场占比 14.7%，排名第 3 | 赛迪顾问 |
| 日志审计系统 | 2018 年度市场占比 10.9%，排名第 1 | 赛迪顾问 |
| 态势感知平台 | 2018 年度市场覆盖排名第 1 | 赛迪顾问 |

*资料来源：公司招股说明书，国盛证券研究所*

**网络信息安全服务和安全平台业务加速增长。**2019 年公司网络信息安全基础产品实现营

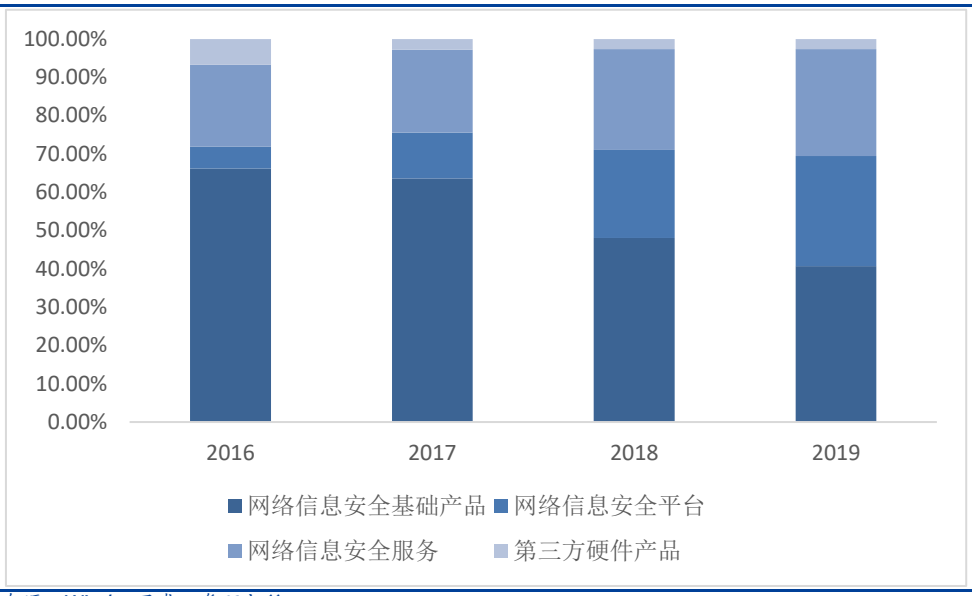
业收入 3.84 亿元，同比增长 29.14%，网络信息安全基础产品占公司营收比重接近 50%，Web 应用防火墙、数据库审计与风险控制系统、综合日志审计平台等产品处于行业领先位置。2019 年网络信息安全平台产品实现营业收入 2.72 亿元，同比增长 91.15%，其中云安全平台产品营收同比增长 176.25%，大数据安全平台产品营收同比增长 62.57%，物联网安全产品同比增长 136.41%。2019 年公司网络信息安全服务实现营业收入 2.64 亿元，同比增长 62.03%，其中 SaaS 云安全服务业务增长迅速。

*图表 5：公司收入构成*

| （单位：亿元） | 2016 | 2017 | 2018 | 2019 |
|---|---|---|---|---|
| **网络信息安全基础产品** | | | | |
| 收入 | 2.08 | 2.70 | 2.97 | 3.84 |
| 增速 | | *30%* | *10%* | *29%* |
| 占比 | *66.17%* | *63.60%* | *48.07%* | *40.68%* |
| 成本 | 0.59 | 0.74 | 0.72 | 0.93 |
| 毛利润 | 1.49 | 1.96 | 2.25 | 2.91 |
| 毛利率 | *71.56%* | *72.46%* | *75.76%* | *75.76%* |
| **网络信息安全平台** | | | | |
| 收入 | 0.18 | 0.51 | 1.42 | 2.72 |
| 增速 | | *184%* | *179%* | *91%* |
| 占比 | *5.70%* | *11.98%* | *22.98%* | *28.78%* |
| 成本 | 0.05 | 0.15 | 0.37 | 0.73 |
| 毛利润 | 0.13 | 0.36 | 1.05 | 1.98 |
| 毛利率 | *74.01%* | *70.45%* | *73.88%* | *72.98%* |
| **网络信息安全服务** | | | | |
| 收入 | 0.67 | 0.92 | 1.63 | 2.64 |
| 增速 | | *36%* | *78%* | *62%* |
| 占比 | *21.43%* | *21.60%* | *26.35%* | *27.97%* |
| 成本 | 0.22 | 0.35 | 0.56 | 0.92 |
| 毛利润 | 0.45 | 0.56 | 1.07 | 1.72 |
| 毛利率 | *67.00%* | *61.50%* | *65.69%* | *64.99%* |
| **第三方硬件产品** | | | | |
| 收入 | 0.21 | 0.12 | 0.16 | 0.24 |
| 增速 | | *-43%* | *35%* | *51%* |
| 占比 | *6.70%* | *2.82%* | *2.61%* | *2.57%* |
| 成本 | 0.18 | 0.11 | 0.15 | 0.22 |
| 毛利润 | 0.03 | 0.00 | 0.01 | 0.02 |
| 毛利率 | *14.06%* | *4.04%* | *7.51%* | *7.51%* |
| **合计** | | | | |
| 收入 | 3.15 | 4.25 | 6.19 | 9.44 |
| 增速 | | *35%* | *46%* | *52.61%* |
| 成本 | 1.04 | 1.36 | 1.80 | 2.81 |
| 毛利润 | 2.10 | 2.89 | 4.39 | 6.63 |
| 毛利率 | *66.87%* | *67.93%* | *70.90%* | *70.19%* |

*资料来源：wind，国盛证券研究所*

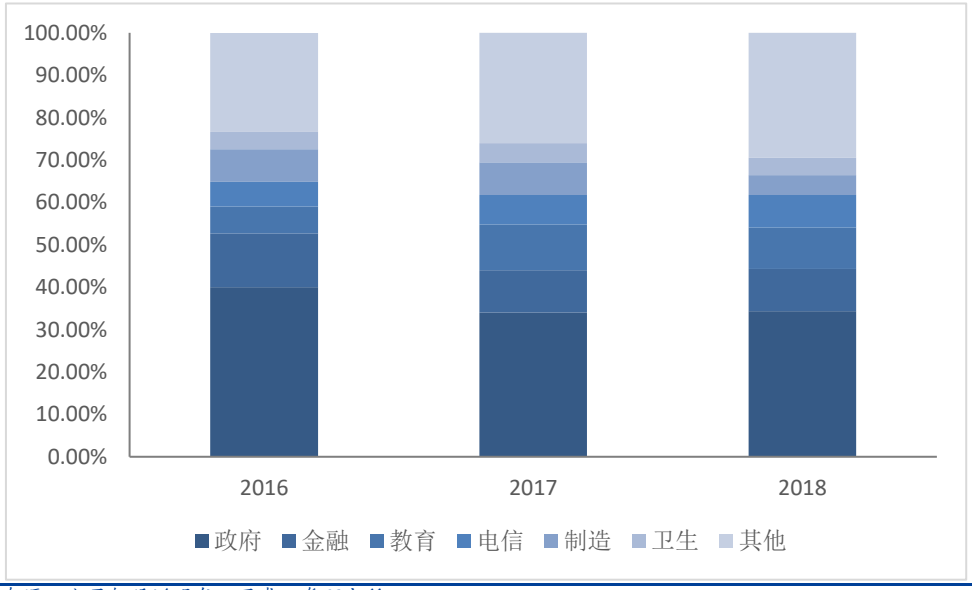
图表 6：公司业务结构




资料来源：Wind，国盛证券研究所

**政府客户贡献收入占比高，下游客户分布分散。**在下游客户方面，公司产品以及服务已经进入了包括运营商、政府、能源、金融、教育、医疗在内的多个行业。其中，公司来自政府部门，尤其是公安部门的订单较多，已为国发委、中国民政部、中国司法部、中国财政部、中国人民共和国公安部、北京公安局、上海公安局等多个行政部门提供网络安全服务。2018 年，来自政府的营业收入共计 2.20 亿元，占比 34.34%，其中来自公安部门的收入占比为 14.95%。先前承接大型活动和会议的经历帮助公司在政府机构中树立了良好的口碑和影响力，且政府市场需求高、潜力大，优质的客户结构保证了公司未来收入的持续增长。

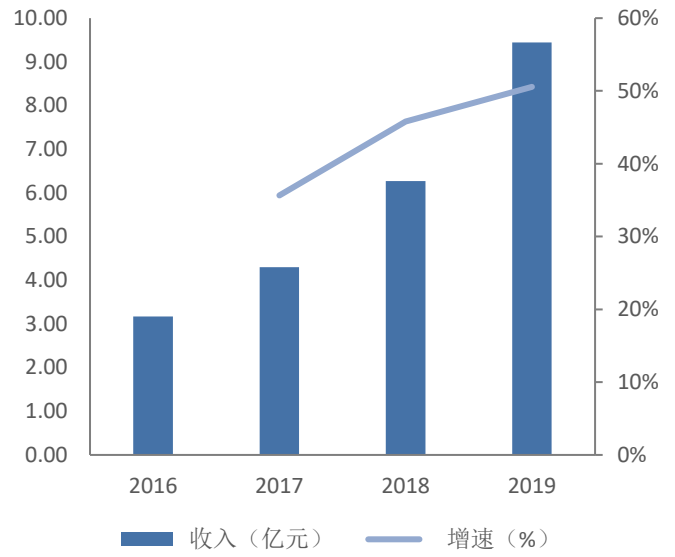
图表 7：下游客户来源




资料来源：公司招股说明书，国盛证券研究所

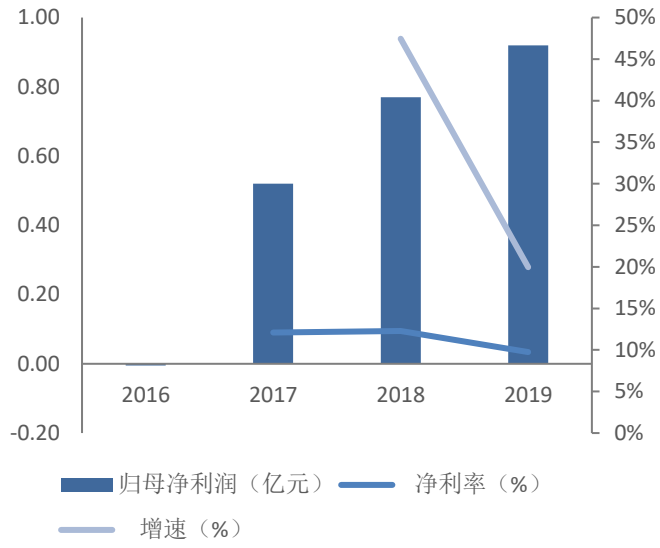
**营收持续高增长，盈利能力逐步提升。**2019 年公司实现营业收入 9.44 亿人民币，同比增长 50.66%，延续了快速增长的趋势。2019 年实现归母净利润 0.92 亿人民币，同比增长 19.96%。

图表 8：公司历年营业收入及同比增长率




资料来源：Wind，国盛证券研究所

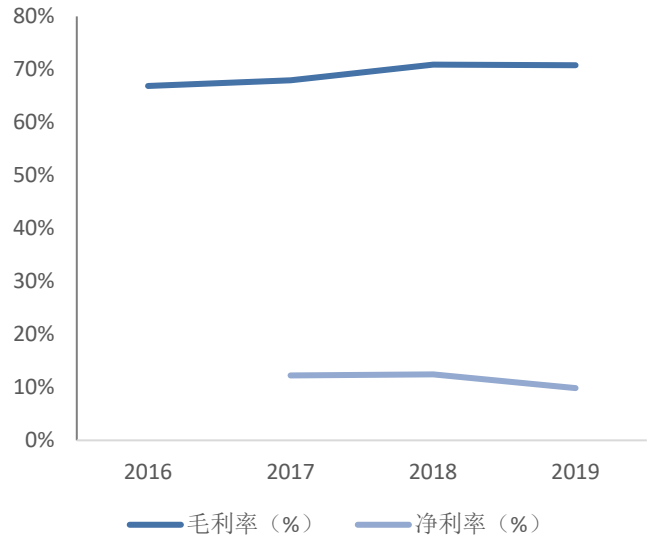
图表 9：公司历年归母净利润及同比增长率




资料来源：Wind，国盛证券研究所

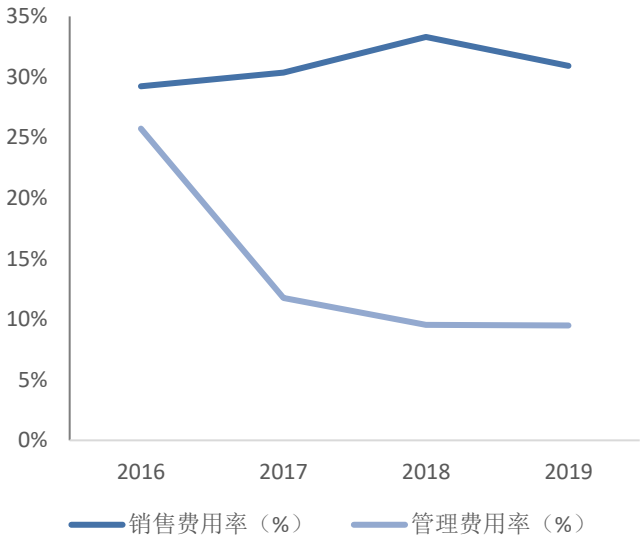
**渠道改善拉动总体毛利率提升，研发持续投入。**公司 2016-2019 年毛利率分别为 67.03%、67.58%、70.50%、69.47%。2016 年和 2017 年公司毛利率基本稳定，2018 年比 2017 年提升了 2.92pcts，主要原因在于公司自 2017 年开始确立渠道政策，加强对渠道商的技术支持，提升渠道商的技术服务能力，从而从整体上减少了公司在渠道模式下的人力投入，致使毛利率提升。公司研发投入持续投入，2019 年研发费用为 2.05 亿人民币，同比增长 34.61%。

图表 10：公司历年毛利率和净利率



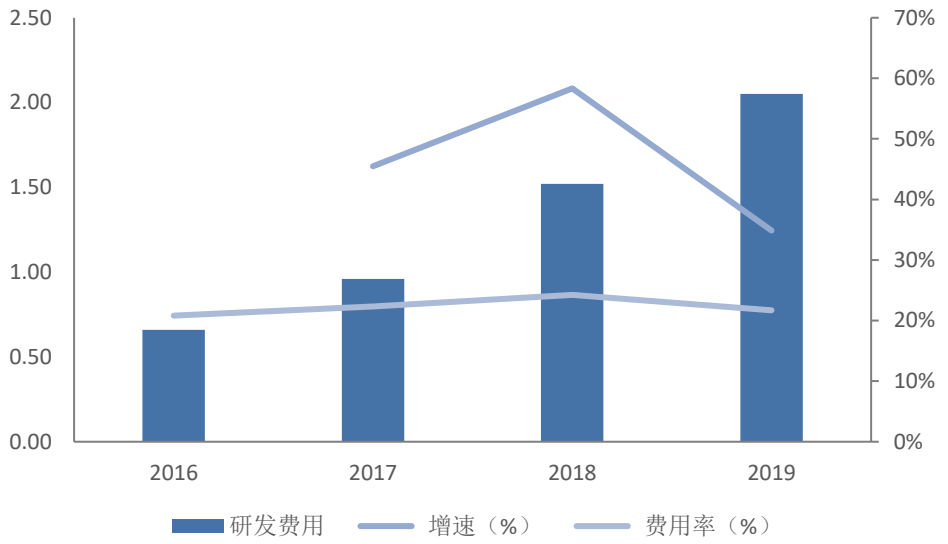

资料来源：Wind，国盛证券研究所

图表 11：公司历年期间费用率




资料来源：Wind，国盛证券研究所

图表 12：公司历年研发投入（单位：万元）



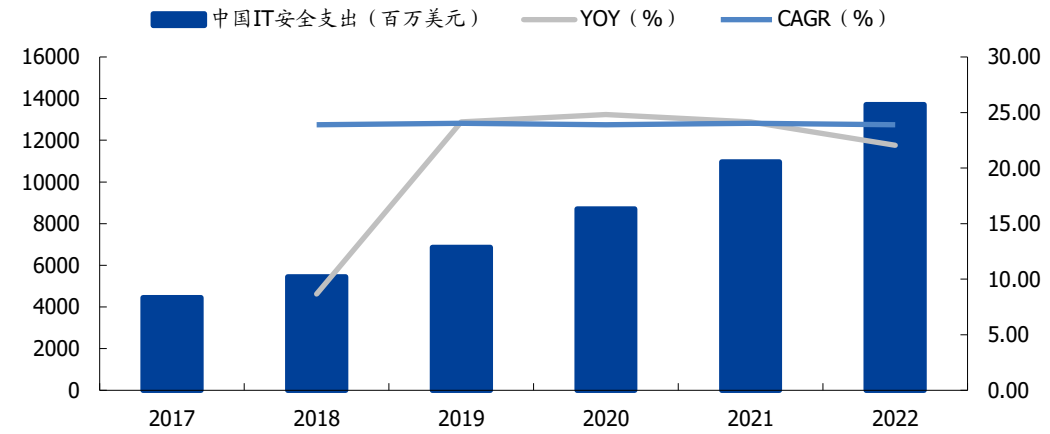

资料来源：Wind，国盛证券研究所

# 安全市场需求强劲，产业向服务主导转型

## 国内安全市场保持高速增长，渗透空间巨大

**国内安全市场未来将维持 25.6%的复合增长。**随着国家对网络安全监管力度的持续加大，中国网络安全市场在未来 3~5 年仍将保持快速发展。IDC 预测，2019 年中国安全解决方案总体支出将达到 69.5 亿美元(不含 IoT 安全)，2018 年~2022 年预测期内的年复合增长率为 25.6%，到 2022 年，市场规模将增长至 137.7 亿美元。

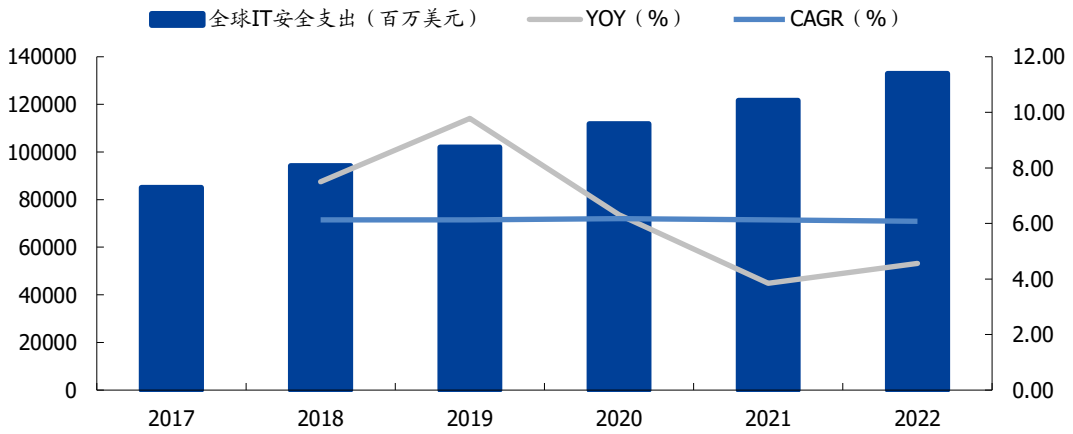
图表 13：中国网络安全市场规模及预测




资料来源：IDC，国盛证券研究所

**全球安全保持平稳增长，中国已成为全球第二大网络安全支出国家。**根据 IDC 预测，2019 年全球 IT 安全相关硬件、软件和服务支出将达到 1031 亿美元，相比 2018 年增长 9.4%。随着全球各行业在安全解决方案上持续投入巨资以应对各种纷繁复杂的恶意威胁，满足各类安全需求，这种快速增长趋势将在未来几年仍将持续。IDC 预测，在 2018-2022 年预测期内，全球安全解决方案支出将实现 9.2%的年复合增长率（CAGR），预计 2022 年将达到 1338 亿美元。

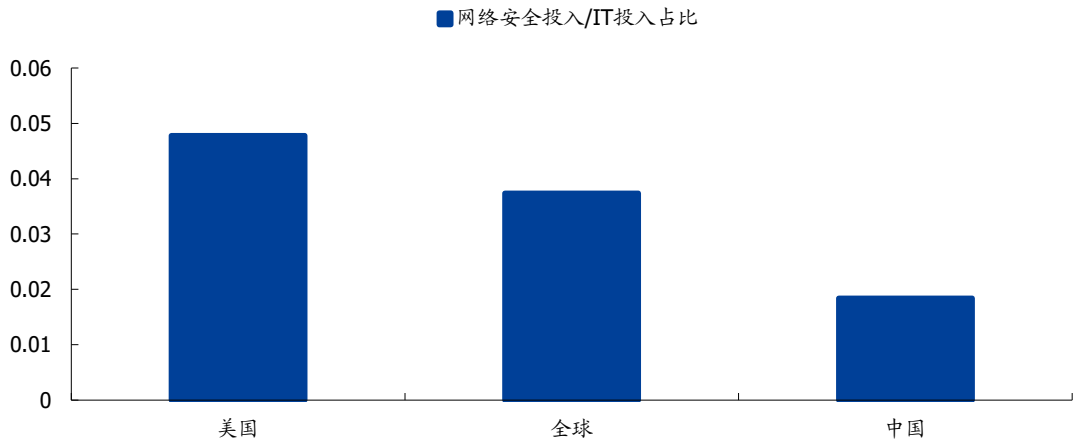
图表 14：全球网络安全市场规模及预测




资料来源：IDC，国盛证券研究所

**中国安全投入/IT 投入占比与全球差距较大，网络安全市场成长空间大。**目前我国对信息网络安全的投入远低于美国以及国际水平。根据 IDC 的统计，2018 年我国对于信息网络安全的投入占信息市场的比例为 1.84%，不到全球水平的 50%，仅为美国水平的 40%左右。随着政府对信息安全越来越重视，我国信息网络安全行业未来有很大的成长空间。

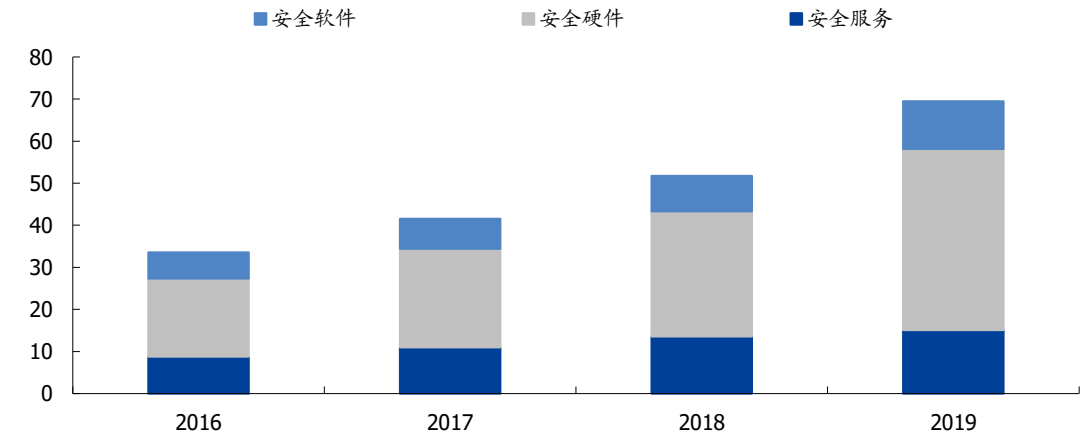
图表 15：中国安全投入/IT 投入占比与全球差距较大（2018）




资料来源：IDC，国盛证券研究所

**安全硬件仍占主导。**2019 年，安全硬件在中国整体安全支出中将继续占据绝对主导地位，占比高达 61.9%；安全软件和安全服务支出比例分别为 16.4%和 21.7%。

图表 16：安全硬件仍占安全市场主导




资料来源：IDC，国盛证券研究所

**政府、通信、金融是安全主要下游，政策是行业主要驱动力。**从行业上来看，政府、通信、金融仍将是中国网络安全市场前三大支出行业，占中国总体 IT 安全市场约六成的比例。随着《国家关键信息基础设施安全保护条例》、数据安全、等级保护 2.0 等相关法律法规的逐步落地，监管部门的监管力度将大幅提升，中国网络安全相关硬件、软件和服务市场将持续保持快速增长，合规性驱动仍将是中国网络安全市场重要的推进器之一。

*图表 17：政府、通信、金融是安全主要下游*


- 2017 年11 月，国务院发布《深化“互联网+先进制造业”发展工业互联网的指导意见》，明确提出我国将从“供给侧”和“需求侧”两端发力，在平台培育、平台试验验证、百万工业企业上云和百万工业App 培育四个方面重点开展工作，加快形成工业互联网平台应用体系。在工业互联网中，工业软件和工业互联网平台是其核心。
- 工业软件安全和工业互联网平台安全是保障《中国制造2025》的根本所在，这直接导致2018年制造业在工业互联网平台上大力投入网络安全建设。

*资料来源：IDC，国盛证券研究所*

## 政策是安全行业主要驱动力，等保 2.0 利好安全服务产品

**网络安全上升为国家战略。**2013 年国家安全委员会成立，2016 年《网络安全法》和《国家网络空间安全战略》相继发布，《网络安全法》是网络空间安全管理方面的基础性法律，填补了在网络安全领域的法律空白，明确了相关责任主体的法律责任及明确的处罚条例，是我国网络法制建设的重要里程碑。《国家网络空间安全战略》第一份关于网络空间安全的战略性文件，对网络空间安全进行全面顶层设计，是指导国家网络安全工作的纲领性文件。2019 年 5 月 13 日公安部发布等保 2.0 细则，2019 年 12 月 1 日实施，公安部牵头组织开展了信息技术新领域等级保护重点标准申报国家标准的工作，等级保护正式进入 2.0 时代。

图表 18：重要网络安全政策梳理

| 时间 | 机构 | 政策 | 内容 |
|---|---|---|---|
| 2013 年 11 月 | 中央国安委 | | 国家安全委员会成立。 |
| 2014 年 2 月 | 网信办 | | 中央网络安全和信息化领导小组成立，提出没有网络安全就没有国家安全。 |
| 2014 年 5 月 | 网信办 | 《加强电信和互联网行业网络安全工作的指导意见》 | 对网络基础设施安全防护、推进安全可控关键软硬件应用、网络数据和用户个人信息保护等做出强调；指出关系国家安全和公众利益的系统使用的重要技术产品和服务，应通过网络安全审查。 |
| 2016 年 11 月 | 全国人大 | 《网络安全法》 | 《网络安全法》审议通过。这是我国第一部网络空间安全管理方面的基础性法律，填补了在网络安全领域的法律空白，明确了相关责任主体的法律责任及明确的处罚条例，是我国网络法制建设的重要里程碑。 |
| 2016 年 12 月 | 网信办 | 《国家网络空间安全战略》 | 第一份关于网络空间安全的战略性文件，对网络空间安全进行全面顶层设计，是指导国家网络安全工作的纲领性文件。 |
| 2017 年 5 月 | 网信办 | 《网络产品和服务安全审查办法》 | 要求党政部门及重点行业优先采购已经通过审查的产品。 |
| 2017 年 6 月 | 全国人大 | 《网络安全法》 | 《网络安全法》正式实施。 |
| 2017 年 7 月 | 网信办 | 《关键信息基础设施安全保护条例（征求意见稿）》 | 《条例》详细阐明了关键信息基础设施的范围、运营者应履行的职责以及对产品和服务的要求，对政府机关，国家行业主管或监管部门，能源、电信、交通等行业，公安机关以及个人进行要求，明确关键信息基础设施范围，规定运营者安全保护的权利和义务及其负责人的职责，要求建立关键信息基础设施网络安全监测预警体系和信息通报制度。 |
| 2018 年 4 月 | 网信办、证监会 | 《关于推动资本市场服务网络强国建设的指导意见》 | 充分发挥资本市场在资源配置中的重要作用，规范和促进网信企业创新发展，推进网络强国、数字中国建设。 |
| 2019 年 5 月 | 公安部 | 《网络安全等级保护条例（征求意见稿）》 | 2019 年 5 月 13 日发布，2019 年 12 月 1 日实施，公安部牵头组织开展了信息技术新领域等级保护重点标准申报国家标准的工作，等级保护正式进入 2.0 时代。 |

资料来源：中国政府网，国盛证券研究所

**如何理解我国网络安全法规？**第一，网络安全政策环境进一步得到优化，在中央网络安全和信息化领导小组的统一领导、统筹协调下，网络安全发展战略、宏观规划和重大政策的制定和实施提上了日程，网络安全保障能力不断增强；第二，网络安全基础工作逐步深化，**主要是关键基础设施风险评估和安全保障、国家网络安全等级保护制度两个方面制度的推进**；第三，网络安全产业保持快速发展，随着网络安全需求日益快速增加，政府、企业、个人在网络安全保障方面的投入都不断增加，产业发展的驱动力仍然强劲。

图表 19：网络安全法规理解

**中央网络安全和信息化委员会成立**

- 2014年2月27日，中央网络安全和信息化领导小组成立，中央网络安全和信息化领导小组办事机构即领导小组办公室

**《中华人民共和国网络安全法》**

- 为保障网络安全，维护网络空间主权和国家安全，社会公共利益，保护公民、法人和其他组织的合法利益，促进经济社会信息化健康发展制定。2016年11月7日发布，自2017年6月1日起施行。

**等级保护2.0标准正式实施**

- 基本要求、设计要求、测评要求
- 同步规划、同步建设同步使用
- 2019年5月13日发布，2019年12月1日实施

**关键信息基础设施安全保护条例（征求意见）**

- 在网络安全等级保护制度基础上，实行重点保护。
- 安全技术措施同步规划、同步建设、同步使用。
- 建立关键信息基础设施网络安全监测预警体系和信息通报制度。

**网络安全战略规划目标**

国家网络安全法律法规政策体系

总体安全策略

国家网络安全等级保护制度、关键信息基础设施重点保护

| 定级备案 | 安全建设 | 等级测评 | 安全整改 | 监督检查 |
|---|---|---|---|---|

| 组织管理 | 机制建设 | 安全规划 | 安全监测 | 通报预警 | 应急处置 | 态势感知 | 能力建设 | 技术检测 | 安全可控 | 队伍建设 | 教育培训 | 经费保障 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|

网络安全综合防御体系

| 风险管理体系 | 安全管理体系 | 安全技术体系 | 网络信任体系 |
|---|---|---|---|

安全管理中心

| 通信网络 | 区域边界 | 计算环境 |
|---|---|---|

等级保护对象

网络基础设施、信息系统、大数据、物联网、云平台、工控系统、移动互联网、智能设备等

本质安全

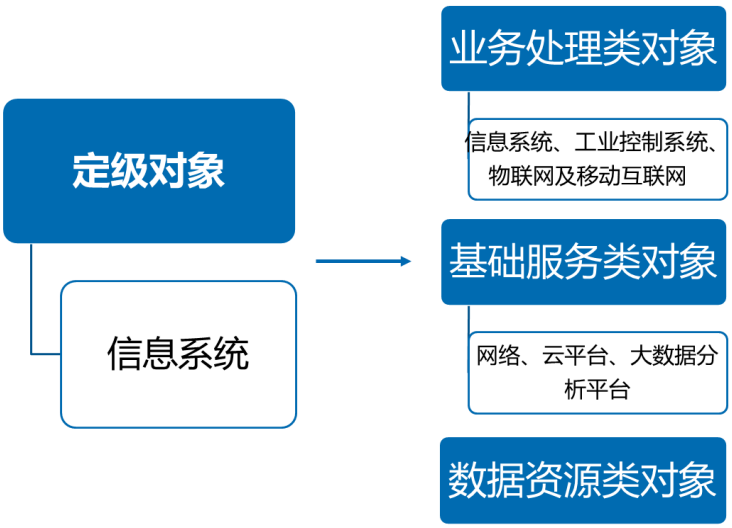
国产CPU、网络、主机、OA、操作系统、应用、中间件、数据库

国家信息安全等级保护政策标准体系

资料来源：2019 网络安全年会，国盛证券研究所

**等保 2.0 相对 1.0 扩宽了监管范围与监管内容：监管范围上从体制内扩展到体制内+具有社会影响力的互联网厂商，乃至全社会主体；监管内容上从企业 IT 系统延伸到了云计算+物联网+车联网+工业控制与移动互联网。**基本要求的内容由一个基本要求变更为安全通用要求和安全扩展要求（含云计算、移动互联、物联网、工业控制）。在 GB/T 22239 网络安全等级保护基本要求合并为五部分：安全通用要求、云计算安全扩展要求、移动互联安全扩展要求、物联网安全扩展要求、工业控制系统安全扩展要求。

图表 20：等保 2.0 扩宽了监管范围与内容




资料来源：天极网，国盛证券研究所

**等保 2.0 标准的推出，促进了态势感知类产品和主动防御市场等安全服务类产品的快速增长。**旧标准更偏重于对于防护的要求，而等保 2.0 标准更适应当前网络安全形势的发展，结合《中华人民共和国网络安全法》中对于持续监测、威胁情报、快速响应类的要

求提出了具体的落地措施。**1.0 和 2.0 最大的区别就是系统防护由被动防御变成主动防御**，以前被动防御的，要求防火墙、杀病毒、IDS，现在要上升到主动防御。

**首先，主动防御体系基本设备有：防火墙、防毒墙、网络版杀毒软件、IPS、准入系统、堡垒机、双因素认证、漏洞扫描器和数据库防火墙。**传统的安全设备防火墙、网络版杀毒软件以及网关层的防毒墙仍是必要的。在等保 2.0 时代，1）需要部署安全准入系统，堡垒机及双因素认证等这类设备，确保接入到网络的人员身份可信，网络出口唯一；2）另外一个基础设备是漏洞扫描器，及时发现漏洞并进行修补；3）数据库防火墙，以前的方案是配备数据库审计、日志审计类设备，这些是操作审计、被动类的设备，不满足主动防御的要求，通过数据库防火墙，实现对数据库的访问行为控制、危险操作阻断、可疑行为审计，从而保障数据的安全。

**其次，需要定期的安全服务：1）**渗透测试服务，通过模拟黑客攻击来主动发现系统可利用的漏洞；2)系统上线前安全测试服务，在新系统上线前对系统进行全面的安全测试，及时发现系统在开发设计时就有的一些安全问题，降低系统带病上线的风险；3)安全运维服务，针对网络及系统定期的进行漏洞扫描，策略检查，安全加固及日志分析等服务，通过安全运维服务，及时发现潜在的安全隐患，寻找有无被黑客攻击的痕迹，及时查漏补缺。

**最后，部署 SOC 平台、安全态势感知平台，从全局性角度去监测、感知、发现整体的安全趋势及可能存在的安全问题。**部署防 APT（高级持续性威胁）攻击的设备发现一些潜在的不定期的隐蔽的各类攻击。

*图表 21：等保 2.0 技术变化简析*

| 分类 | 安全控制点 | 等保三级要求内容 | 应对思路 |
|---|---|---|---|
| 网络和通信安全 | 入侵防范 | c）应采取技术措施对网络行为进行分析，实现对网络攻击特别是未知的新型网络攻击的检测和分析 | 部署安全防护设备能够对新型网络攻击进行检测和分析，对未知威胁检测需具备云端未知威胁分析引擎，并实现本地防护设备能与云引擎进行联动的功能，**具备与云引擎联动分析的下一代防火墙或安全感知平台可满足此要求** |
| | 集中管控 | f）应能对网络中发生的各类安全事件进行识别、报警和分析 | 部署能够**对网络中发生的各类安全事件进行识别、报警和分析**的安全防护设备可以满足此要求，如**安全感知平台** |
| | 边界防护 | c）应能够对内部用户非授权联到外部网络的行为进行限制或检查 | 对从内到外网络的行为进行限制或检查，传统防火墙无法满足此类要求，必须采用具有**双向检查能力的新一线防火墙**或上网行为管理检测非法无线共享满足 |
| | | d）应限制无线网络的使用，确保无线网络通过受控的边界防护设备接入内部网络 | 必须在无线网络边界增加安全防护设施 |
| | 安全审计 | e）应能对远程访问的用户行为，访问互联网的用户行为等单独进行行为审计和数据分析 | 新增对远程访问用户及互联网访问用户行为单独进行审计分析，数据中心的服务器如果可以访问互联网或需要进行远程管理或访问，需要在互联网出口单独部署上网行为管理或 VPN |
| 设备和计算安全 | 入侵防范 | e）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警 | 应在**重要节点部署检测探针**，能够检测到入侵行为，将**日志汇总到安全感知平台进行分析**，并在发生严重入侵事件时提供报警 |

*资料来源：天极网，国盛证券研究所*

图表 22：等保 2.0 主动防御体系具体部署设施

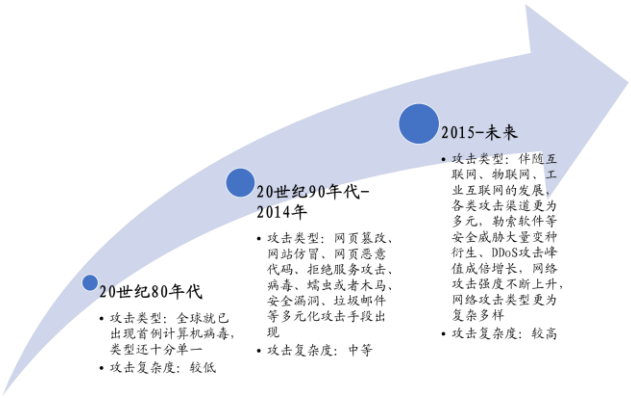

资料来源：天极网，国盛证券研究所

**《国家关键信息基础设施安全保护条例》或年底出台。**在 2019 C3 安全峰会上，公安部网络安全保卫局总工郭启全表示：“由中央网信办和公安部双牵头的《国家关键信息基础设施安全保护条例》（以下简称《条例》）已上报国务院，等待批准之后将会发布实施，《条例》将为关键信息基础设施保护提供强大的支撑和保障。”《条例》有望年内正式发布。郭启全明确表示，中央网络安全和信息化委员会是保护关键信息基础设施安全的领导机关；中央网信办和公安部是保护关键信息基础设施安全的牵头部门；关键信息基础设施的运营者是关键信息基础设施安全的主责部门。《条例》将覆盖电信、广播电视、能源、金融、交通、铁路、航空、卫生健康、社会保障、关键制造、电子政务、化工、国防科技等领域的重要网络、重要信息系统、云平台、物联网、工控系统、大数据中心、大型公共服务平台等。同时，在网络安全行动层面，公安部近期组织了“净网行动”“护网行动”两大行动，切实保卫国家关键信息基础设施安全。

## 安全产业向服务主导转型，云安全服务将成为细分潜力最大的安全市场

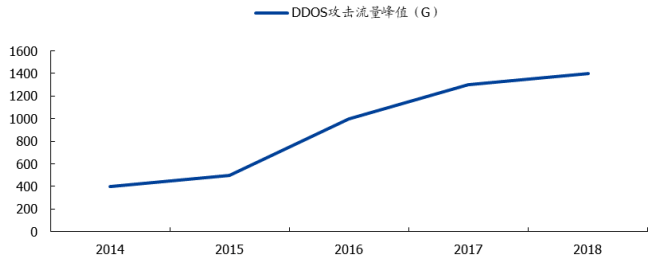
**网络安全攻击逐年增加，攻击方式越发多元化、复杂化。**近年来，我国网络安全攻击逐年增加，根据国家互联网应急中心统计，2018 年我国境内感染计算机恶意程序的主机数量达到 655 万个，同比有所下降；移动互联网恶意程序捕获数量 283 万个，5 年间增长 197.6%；国家信息安全漏洞共享平台收录安全漏洞数量 14,201 个，5 年间增长 55.0%。伴随互联网的高速发展及物联网、工业互联网、云计算、大数据等新兴领域和新兴技术的快速发展，网络攻击形态更为复杂。根据赛迪调查显示，国内 DDoS 攻击每天平均攻击次数近千次，从 DDoS 攻击流量带宽分布情况来看，当前 85%的攻击为 100G 以下的流量攻击，但超过百 G 的攻击累计占总攻击次数比重在逐步上升，同时伴随互联网宽带提速、物联网、IPV6 的发展使 DDoS 攻击峰值流量持续攀升，2018 年 DDoS 攻击流量峰值已经达到了 1.4T，预计 2020 年将接近 2T。

图表 23：网络攻击演变历程




资料来源：赛迪，国盛证券研究所

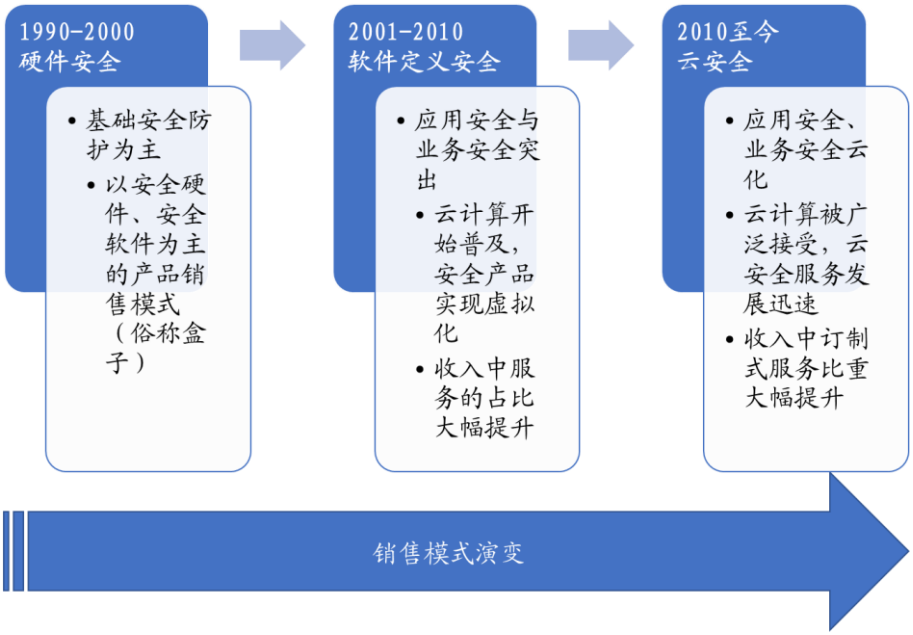
图表 24：2014-2018 年 DDoS 攻击流量峰值情况




资料来源：赛迪，国盛证券研究所

**安全服务是长期发展方向。**在 20 世纪 90 年代，为了应对信息高速公路带来的流量压力和安全问题，传统企业硬件防火墙产品开始普及；从 21 世纪初开始，社交网络与云计算开始兴起，带来了对于网络应用安全的强烈需求，应用安全厂商快速成长；步入 2010 年后，顺应云计算的要求，安全设备逐渐实现虚拟化，催生了下一代防火墙、安全可视化、云安全等新兴产品。从 2013 年开始，软件即服务（SaaS）开始得到广泛认同，安全产品被以 SaaS 的方式提供给客户，云安全服务获得更快的客户积累与收入增长，云安全服务厂商以技术实力和渠道拓展获得了飞速发展，已成为欧美网络安全巨头的必争之地。

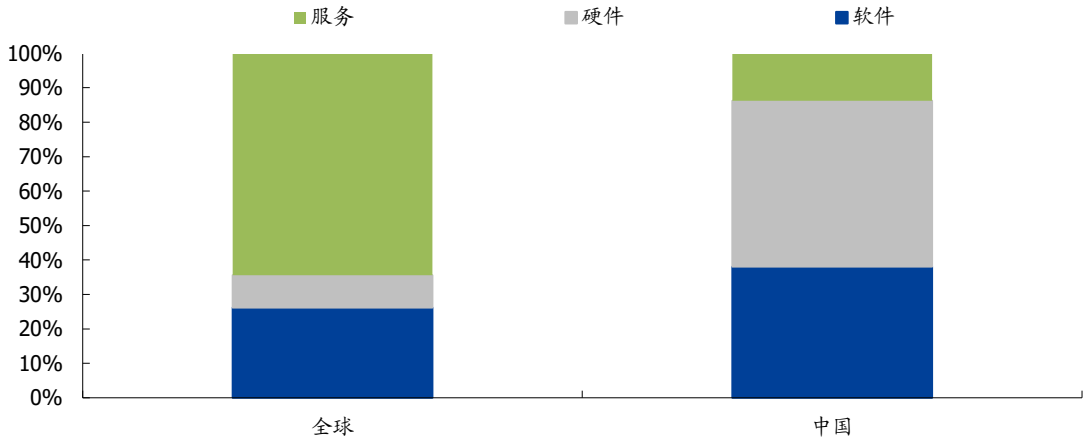
图表 25：美国网络安全在商业模式上的演变路径




资料来源：Gartner，赛迪，国盛证券研究所

**网络安全产业正由产品主导向服务主导转型，**云安全服务等新技术、新业态层出不穷，网络安全技术密集化、产品平台化、产业服务化等特征不断显现。随着 IT 虚拟化的转型和云服务理念的渗透，中国的网络安全行业将向国际看齐，安全服务是长期发展方向，预计未来，中国网络安全服务市场份额得到更快提升，网络安全服务市场有望成为未来亮点。

图表 26：2018 年全球与中国网络安全市场结构对比




资料来源：Gartner，赛迪，国盛证券研究所

**中国云安全服务生态逐渐形成。**中国云安全服务业的发展略晚于美国市场 2-3 年，即 2011 年萌芽，2014 年众多技术驱动的创业型公司加入到该领域，同时 2014 年阿里云等公有云厂商正式上线云安全服务，行业逐渐进入快速发展阶段。到 2018 年，云安全良性生态逐渐形成，包括公有云和政企私有云。随着云技术的普及应用，云安全服务快速发展，基于自动化、远程化、智能化的威胁监测、攻击防御等新兴服务模式也逐步得到推广和应用，带动了网络安全市场服务化转型。2018 年，行业出现更多针对云管理平台、工作负载和企业 SaaS 应用的攻击。各安全企业纷纷布局云安全防线，切实提供云服务安全应用，保护包含用户信息的应用及服务免予侵扰。

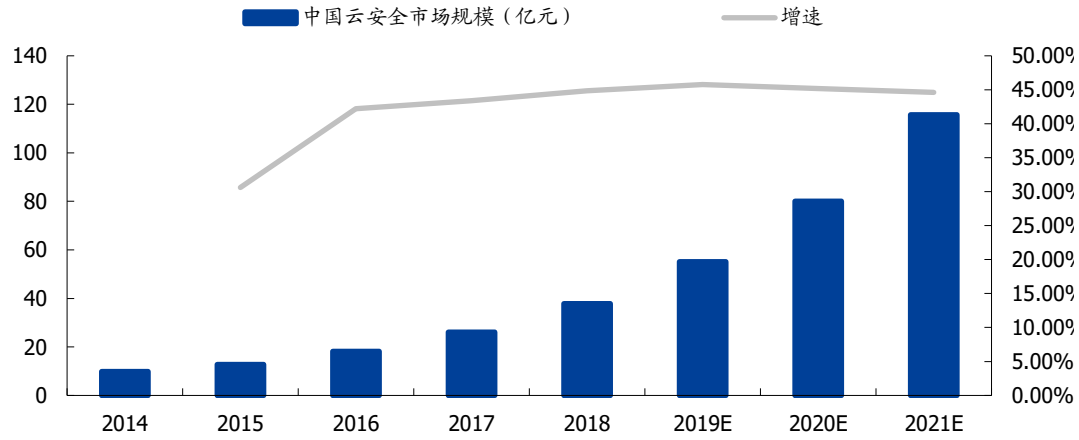
图表 27：中国云计算与云安全发展历程简略图


资料来源：Gartner，赛迪，国盛证券研究所

**云安全服务将成为细分潜力最大的安全市场。**根据赛迪统计，2018 年，中国云安全服务市场规模达到 37.8 亿元，同比 2017 年增长 44.8%，中国云安全服务市场处于爆发式增长阶段。随着国家对网络安全的重视、互联网产业的高速增长和伴随互联网发展而来的日趋严峻的安全问题，以及云计算、5G、大数据、物联网、工业互联网、人工智能等新技术、新应用的发展，针对于环境的虚拟化安全产品具有广阔发展前景，中国云安全整体的市场规模会随云计算市场增长而快速崛起。预计到 2021 年中国云安全服务市场规

模将达到 115.7 亿元，未来三年年均增长率为 45.2%，行业正处爆发式增长趋势。

*图表 28：2014-2021 年中国云安全服务市场规模及预测*




*资料来源：赛迪，国盛证券研究所*

## 5G 多样化场景与技术革新带来安全增量

**网络安全问题愈发突出。相比于 3G/4G 网络，5G 应用场景中将接入大量物联网设备和第三方企业应用，因此 5G 将面临更加突出的安全问题。**高速率低时延将成为一把双刃剑，一方面给用户带来较好的体验，另一方面也意味着网络攻击速度更快，破坏力更大。具体来看，5G 将面临以下两方面的安全挑战：

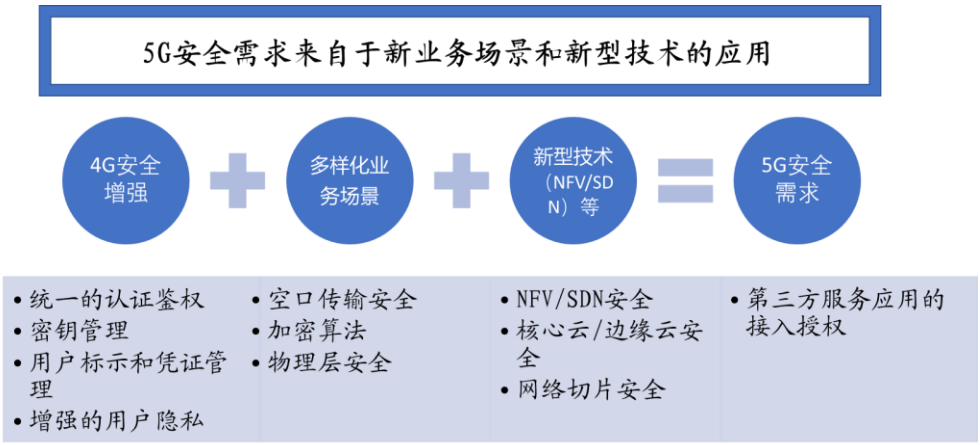
**一是安全需求更加多样。**5G 应用场景更加多元，行业应用对所有环境信息有加密的需求，而个人用户重点关注关键信息加密情况。不同用户的安全需求不同，需要加快 5G 安全多样化布局。例如，对于自动驾驶、远程控制，在通信过程中如果受到安全威胁则可能会危及生命，为避免车辆碰撞需要高级别安全措施，且不能额外增加通信时延。

**二是“信令风暴”或将更加频繁。**随着越来越多的 IoT 设备接入 5G 网络，海量物联网终端发起的“信令风暴”将引发网络拥塞甚至崩溃。物联网设备安全需求多样，需要降低物联网设备在认证和身份管理方面的成本，支持物联网终端低成本、高效海量部署，因此相关业务需要轻量级安全算法和高效简单安全协议来保障应用安全。

面对新的挑战，5G 安全机制要在满足基本通信安全的基础上，为不同业务场景提供差异化安全服务，要能够适应多种网络接入方式及安全构架，注重用户隐私保护，支持提供开放的安全能力。

因为，5G 带来的安全增量包括，**1）4G 安全的增强外；2）多样化的业务场景：空口传播安全、加密算法、物理层安全；3)新型技术（NFV/SDN/网络切片）带来的安全需求：NFV/SDN 安全、核心云/边缘云安全、网络切片安全；4）5G 安全需求：第三方服务应用的授权。**

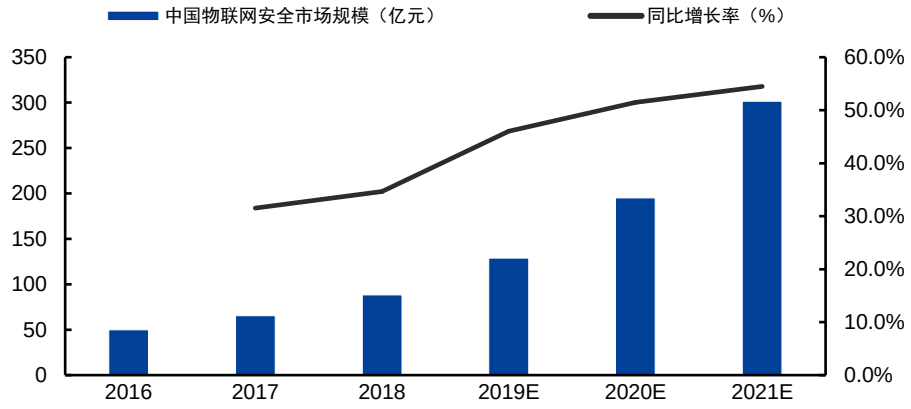
图表 29：5G 带来的安全增量




资料来源：2019 网络安全年会，国盛证券研究所

**物联网安全具备百亿市场规模。**根据赛迪顾问《2019 中国网络安全发展白皮书》，2018 年中国物联网安全市场规模达到 88.2 亿，增速高达 34.7%，明显高于行业平均增速。物联网设备存在着系统性安全缺陷和隐私风险，导致物联设备大规模“变砖”的恶意软件大量存在等等因素，将导致未来很长一段时间，物联网安全威胁都将是最大的安全威胁之一，物联网安全支出在信息安全整体市场的占比也将快速提升

图表 30：中国物联网安全市场规模及增速




资料来源：赛迪顾问，国盛证券研究所

# “战略+技术”成就产品高增长，引领安全服务演绎新模式

## 态势感知、云安全、AiLPHA 大数据持续推动平台高速增长

### 态势感知平台：市场的领导者

**公司是公安和网信行业态势感知的主要建设者和推动者。**公司从 2015 年开始参加公安部最初的感知平台规划，并成为主要的技术支持单位。公司参与了多项态势感知行业和国家标准的制定，也是业内少数能够提供从底层数据采集、处理、存储、分析挖掘和上层业务应用建设全方位建设能力的企业。公司的态势感知平台主要面向政府、网信、公安、行业主管单位及大型企事业单位，设计了等级保护管理、实时监测、态势感知、通报预警、应急指挥、情报管理、追踪溯源等功能，是具有综合安全事件分析与全局安全

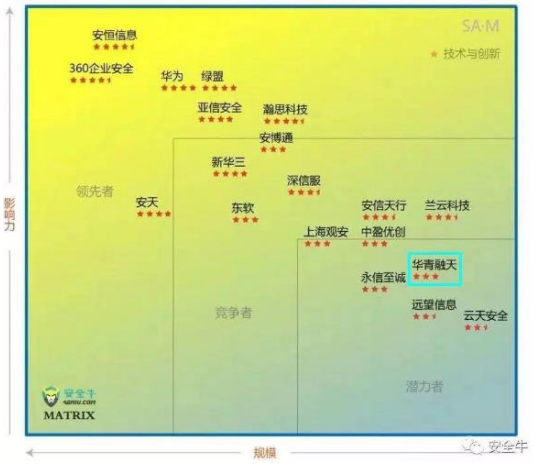
感知能力的安全管理平台。在日常运营使用过程中，平台可与专用监管工具联动，极大简化了监管部门日常检查工作流程。同时，平台配套了安全服务与数据情报服务体系，全面应对各种安全管理场景。

*图表 31：网络安全态势感知通报预警平台框架结构*


*资料来源：公司官网，国盛证券研究所*

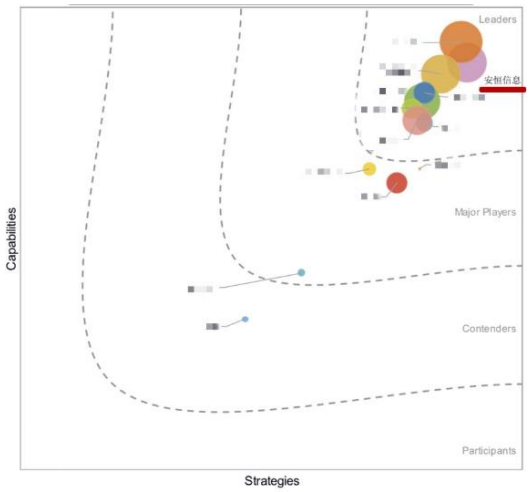
**公司态势感知产品以优秀的技术、丰富的实践以及领先的市场战略，成为中国态势感知解决方案的领导者企业。**在 IDC 发布的《中国态势感知解决方案市场 2019 年厂商评估》中，公司被评选为态势感知领导厂商，其中战略能力排名第一，市场份额排名第二。公司凭借在多源异构数据采集、海量数据存储、安全事件溯源分析、安全态势可视化展示、多场景业务监管等方面的优势，成为领导者企业。此外，在安全牛发布的态势感知矩阵内，同样以先进的技术和优秀的业务进入领导者企业。

*图表 32：安全牛态势感知矩阵*




*资料来源：安全牛，国盛证券研究所*

*图表 33：IDC MarketScape：中国态势感知解决方案市场厂商评估*




*资料来源：IDC，国盛证券研究所*

**领先的技术和优质的服务将维持公司较强和行业竞争力。**从产品本身来看，平台支持不同种类的安全数据采集设备，并基于大数据关联分析，形成网络空间全方位全要素的安全数据采集分析能力。领先的可视化技术，使得用户对网络中存在的威胁和异常清晰可见。此外，平台支持多种终端设备访问，使得用户可以即时得知重要的网络安全事故。平台亦通过大数据对比加强了对 0day 病毒的识别和系统保护，有效保护了用户的网络安

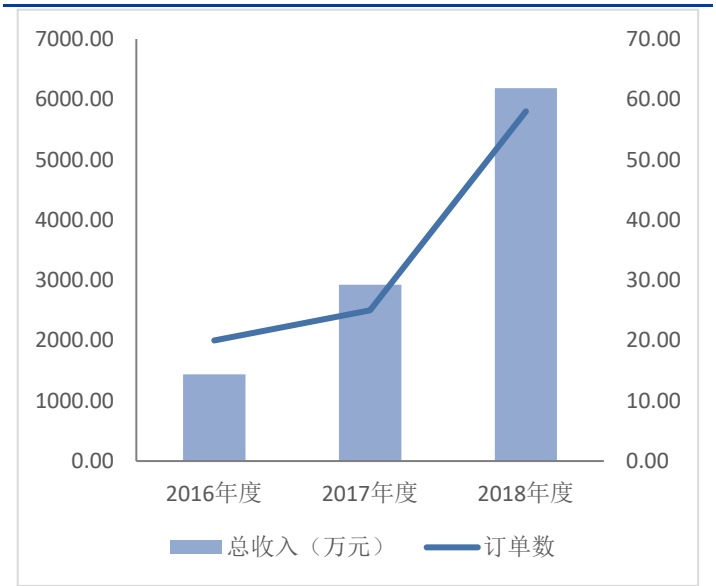
全。从公司服务来看，公司提供 7X24 小时在线的专家服务，并基于公司庞大的安全分析专家和安全服务团队，提供“云+平台+服务”的运营模式，为用户提供及时有效的安全服务，为业务不间断稳定运行提供安全保障。

图表 34：态势感知产品特色


资料来源：公司官网，国盛证券研究所

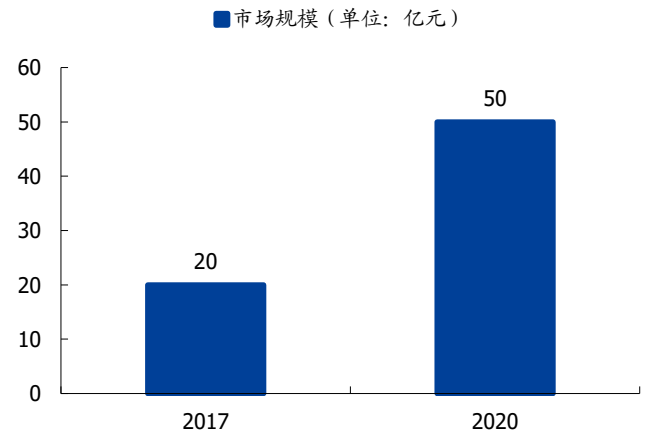
**态势感知业务发展迅速，承接大订单的能力增强，随着平台产品的成熟、态势感知市场的快速发展，公司该业务仍有提升空间。**公司 2018 年承接态势感知预警平台订单 58 个，实现收入 6186.88 万元，同比增长 112%，态势感知业务发展迅速。根据安全牛《中国网络安全细分领域矩阵图》，2017 年我国态势感知市场规模约 20 亿元，预计 2020 年态势感知整体市场规模将超过 50 亿元，CAGR 达 35.72%，市场保持高速增长，公司作为行业的领先企业，未来增长可期。

图表 35：公司历年态势感知订单数及收入




资料来源：招股说明书，国盛证券研究所

图表 36：中国态势感知市场规模预测




资料来源：招股说明书，国盛证券研究所

## AiLPHA 大数据智能安全平台：智能安全运营新模式

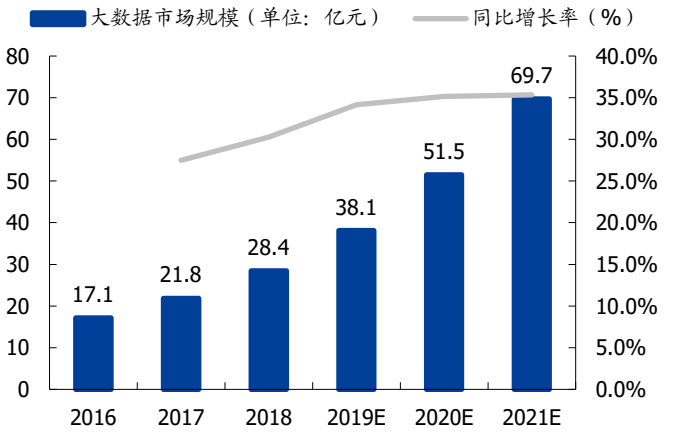
**AiLPHA 大数据智能安全平台以“AI 驱动安全”为核心理念**，集成超大规模存查、大数据实时智能分析、用户行为（UEBA）分析、多维态势安全视图、企业安全联动闭环等安全模块，为客户提供全局态势感知，保障业务不间断稳定运行。

图表 37：AiLPHA 大数据智能安全平台产品架构


资料来源：公司官网、国盛证券研究所

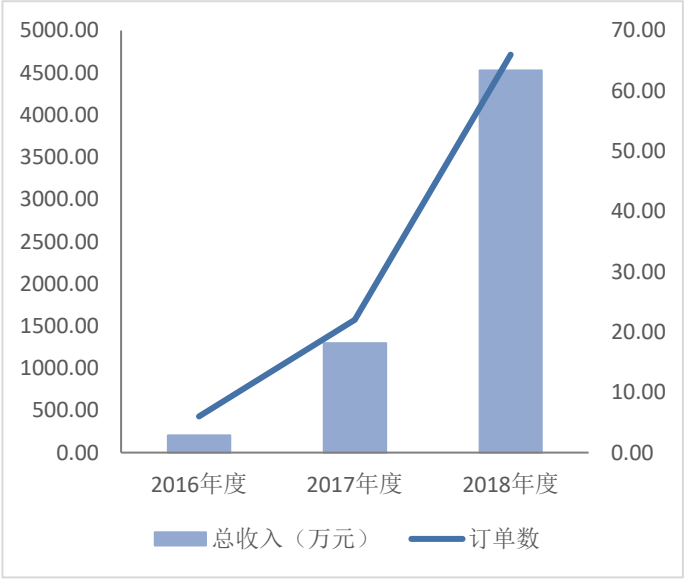
**大数据平台业务增长迅速。**公司 2018 年签订 AiLPHA 大数据智能安全平台订单 66 个，实现收入 4526.61 万元，同比增长 249%，业务发展维持高速增长。根据赛迪顾问发布的《中国网络安全发展白皮书（2019）》，2021 年中国大数据市场规模可达 69.7 亿元，根据这个数字，大数据市场 CAGR 可达 35.26%，仍有相当大的发展空间。公司作为国内较早布局大数据行业的网络安全公司，具有一定的先发优势，以往积累的口碑和销售渠道将有转化为新增顾客的可能，业务将会迎来确定性增长。

图表 38：中国大数据市场规模




资料来源：招股说明书、国盛证券研究所

图表 39：公司历年大数据订单数量及收入




资料来源：招股说明书、国盛证券研究所

**AiLPHA 大数据智能安全平台开启智能安全新生态运营。**AiLPHA 大数据智能安全平台在金融、医疗、公安、大数据局等方面持续渗透，基于大数据技术的新一代安全架构，帮助客户构建以”安全要素管理、大数据关联分析、可编排的安全运营和管理”为三大核心技术支撑的智能安全运营体系；技术拓展层面，公司联合大数据网络安全态势感知及智能防控技术国家地方联合工程研究中心、江之恒网络信息安全研究中心，开展 SOAR、UEBA、ATT&CK、数据安全管控、数据安全交换共享等前沿安全技术研究，形成并申请相关专利 80 余件，并获得以 Breakout Security Information Event Management (SIEM) InfoSec Award for 2019、2019 世界人工大会智能产业安全十大创新实践为代表的 16 项荣誉，逐渐形成以 AiLPHA 大数据智能安全平台为核心的智能安全运营新生态建设，打造以智能检测、智能溯源、智能响应以及特殊时期重大活动保障为一体的智能安全运营新模式。

## 云安全：公有云、私有云、多云混云安全方案全面部署的第三方厂商

**公司云安全主要专注于公有云安全、私有云安全和 SaaS 安全服务三个部分：**

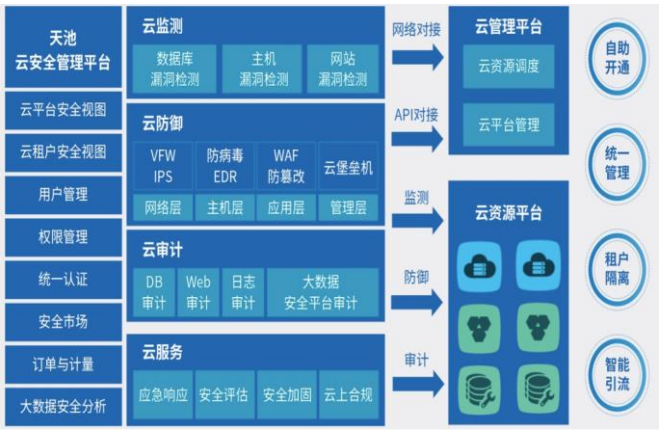
**公有云领域：为阿里云等十多家国内外主流公有云平台提供安全服务。**公司 2015 年开始与阿里云合作，是阿里云安全市场首批安全供应商之一。目前，公司云堡垒机、云数据库审计等相关产品累计保护数千家云上企业用户，云堡垒机服务和保护的云主机更是达到了十几万台以上。目前公司的云安全产品已在阿里云、腾讯云、华为云、AWS 亚马逊、中国电信天翼云、中国联通沃云等十多家国内外主流公有云平台提供安全服务。

**私有云领域：推出天池安全管理平台。**2016 年，公司推出天池安全管理平台，该平台是公司结合自身在安全领域多年的经验及技术积累，打造的专门针对云上安全的安全产品，覆盖了云检测、云防御、云审计、云服务等一系列模块，可以为私有云用户提供一整套的云安全解决方案和城市级云安全运营方案。目前，天池安全管理平台已经在 50 多个省市的政务云、警务云上运行，为公司积累了良好的口碑。

*图表 40：18 类云安全能力*


*资料来源：公司官网、国盛证券研究所*

*图表 41：平台为用户提供便捷的统一管理平台*




*资料来源：公司官网、国盛证券研究所*

## 安全服务：一切产品皆资源，一切资源皆服务

**SaaS 云安全服务业务增长迅速。**公司积累了大量活跃在线试用用户群体，形成了以玄武盾为核心的云防护、云监测服务、以安全数据大脑为核心的情报订阅、行业监管 SaaS 服务模式，成功的为多个省市的政务云、政府网站群、政府在线系统提供了 7*24 小时云安全服务。在专家服务方面，公司作为国家级重大活动网络安全的核心保障力量，在 2019 年承接参与了 20 多场国家级安保任务，包括 2019 世界互联网大会、中华人民共和国建国 70 周年、第七届世界军人运动会、第二届中国国际进口博览会等，成功实现 0 安全事故，累计投入专家 1000 余人，累计拦截各类网络攻击超过 1 亿次，收到客户 100 多封感谢信，用自己的实际行动展示公司的专业性、责任心和使命感。

图表 42：玄武盾云防护框架结构


资料来源：公司官网、国盛证券研究所

**城市安全运营中心服务为城市建设安全大脑平台。**在智慧城市服务方面，公司快速组建优势团队布局新一轮智慧城市发展机遇，积极参与各地城市大数据平台（城市大脑）项目建设，为上海、江苏、山东、内蒙古、杭州等省市大数据平台建设提供了安全保障服务。同时公司以体系、平台、人才赋能，三位一体的打造“智慧城市安全运营中心”，通过网络安全体系架构和运行机制的改造、“大数据+安全智能”为核心的安全大脑平台建设、本地化专业安全服务团队的组建，构建城市级网络安全保障机制，实现区域关键信息基础设施、党政机关和企事业单位重要信息系统、工业互联网设施的全方位保护，统一集中运营管理及常态化的威胁发现和应急处置，提高城市管理者决策的科学性和精准性，实现用“数据说话、用数据决策、用数据管理”的城市安全管理新模式。

图表 43：智慧城市“安全大脑”解决方案


资料来源：公司官网，国盛证券研究所

**网络安全服务正在走向第五代服务模式，数据驱动即服务，强依赖自主运营的智能服务。**网络安全服务正在朝着数据化、智能化、自动化、集约化、实战化、闭关化的趋势演进，它意味着非接触式在线新经济场景下将向着整合了 SaaS、远程运维、AI 智能分析、威胁情报、专家经验的 4.5G 安全服务的方向发展。简单地说，就是安全能力的服务化。

图表 44：网络安全服务在向安全能力的服务化演进


资料来源：2020 西湖论剑·网络安全线上峰会，国盛证券研究所

**“一切产品皆资源，一切资源皆服务”。**未来第五代安全服务面会更广、效能会更高，代表着网络安全今后一个重要的走向。软件即服务、情报即服务、AI 即服务、平台即服务以及数据安全即服务，加上专家经验，将会形成大的应用场景和大运营中心，必将为数字经济和新基建起到更好的保障作用并带来更大的价值。

图表 45：一切产品皆资源，一切资源皆服务


资料来源：2020 西湖论剑·网络安全线上峰会，国盛证券研究所

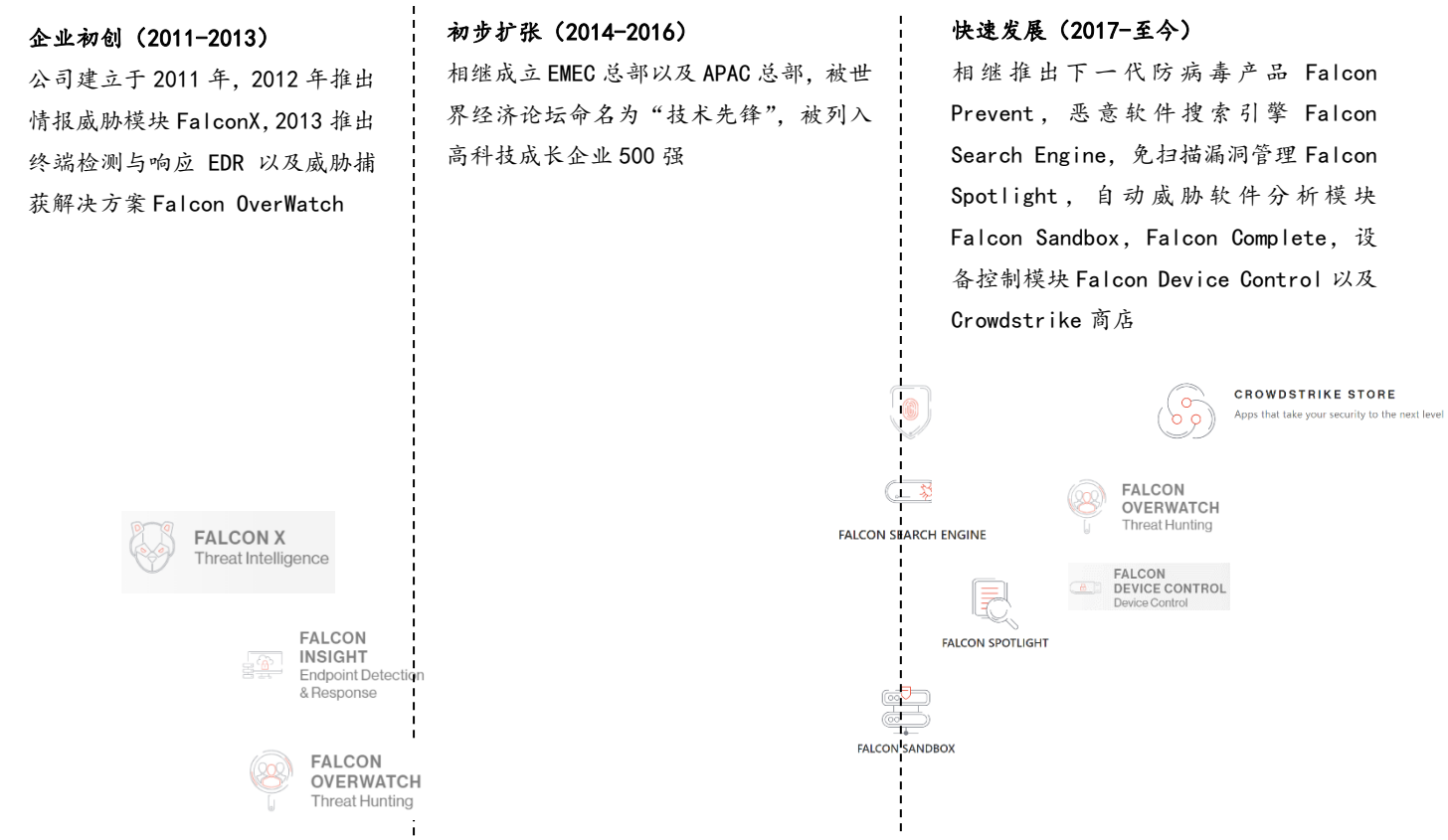
# CrowdSrike：快速进化的终端安全的 SaaS 龙头

## 终端安全 SaaS 龙头，产品线扩张拉动收入高速增长

**CrowdStrike 终端安全 SaaS 龙头。**创立于 2011 年，是一家专注于终端安全的厂商。公司经过八年发展，已经成为全球终端安全市场的领军企业，并于 2019 年 6 月在纳斯达克鸣钟上市。公司通过应用人工智能、云计算、图储存系统等计算技术分析大数据，进而识别网络安全威胁。自 2017 年至今，公司在 Gartner、IDC、Forrester、NSS 等多个第三方权威机构的行业评估结果中名列前茅，验证了其产品的技术性和影响力。

**产品线不断扩张助力公司不断发展。**公司由前迈克菲 CTO 创立，并在 2012-2013 年相继推出拳头产品情报威胁模块 Falcon X 以及终端检测与响应产品 Falcon Insight。2017 年，公司进一步拓展产品线，先后发布推出下一代防病毒产品 Falcon Prevent，恶意软件搜索引擎 Falcon Search Engine，免扫描漏洞管理 Falcon Spotlight，自动威胁软件分析模块 Falcon Sandbox,Falcon Complete 以及设备控制模块 Falcon Device Control，2019 年推出 Crowdstrike 商店，拓展 PaaS 业务。

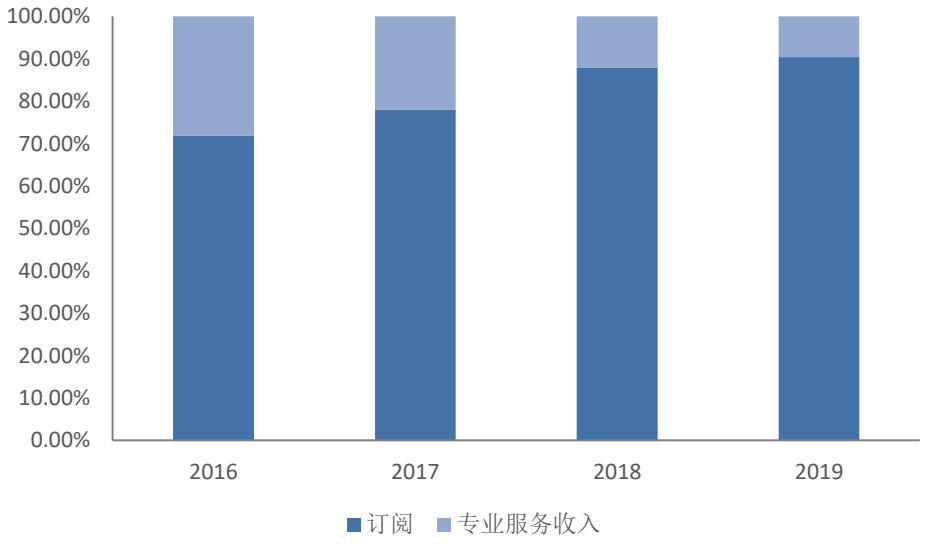
图表 46：Crowdstrike 发展历史（单位：万元）




资料来源：公司官网，国盛证券研究所

**公司订阅收入占比逐年提高。**公司收入分为订阅和专业服务两部分，2019 年实现营收为 30.05/3.11 亿，订阅收入占比逐年提高：1）订阅服务完全基于 SaaS 方式提供，内容为 Falcon 平台内三个产品线，分别为终端安全、安全和 IT 运营、情报威胁下的 10 个服务模块，是公司近几年的增长点；2）专业服务包括事件响应服务、网络安全成熟度评估、渗透测试等，主要作为 Falcon 平台云模块的配套销售。

图表 47：Crowdstrike 收入结构

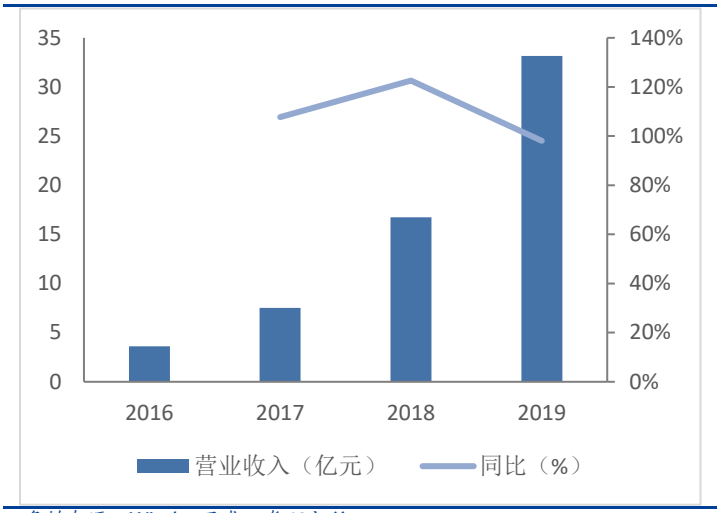



资料来源：Wind，国盛证券研究所

**营收持续高速增长。**公司 2016-2019 年分别实现营收 3.62、7.52、16.74、33.16 亿元，

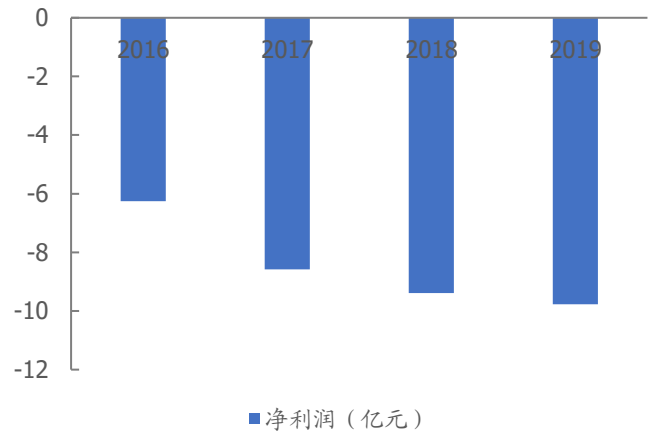
同比增长 125.1%、110.4%、92.7%，营收持续高速增长。2016-2019 实现净利润-6.26、-8.58、-9.39、-9.77 亿人民币，公司持续加大投入。

图表 48：Crowdstrike 历年营业收入




资料来源：Wind，国盛证券研究所

图表 49：Crowdstrike 历年净利润




资料来源：Wind，国盛证券研究所

## 如何成就终端保护龙头？

**基于云端部署的 SaaS 服务带给予了 Falcon 平台在灵活性、有效性、可拓展性方面的竞争优势。**公司目前在 Falcon 平台上集成了 10 个云模块，覆盖终端安全、IT 运维、情报威胁等多个板块。通过订购服务的方式，顾客可以按照付费档次灵活地选择所需的服务。目前，公司提供四个档次的订购服务：

1）Falcon Pro（专业版），包括下一代防病毒产品 Falcon Prevent 以及情报威胁模块 Falcon X；

2）Falcon Enterprise（企业版），在专业版的基础上新增了终端检测与响应产品 Falcon Insight、设备控制模块 Falcon Device Control 以及威胁解决捕获方案 Falcon Overwatch；

3）Falcon Premium（高级版），在企业版的基础上新增了 IT 卫士 Falcon Discover；

4）Falcon Complete（完整版），提供专业人员的定制服务。

除了订购服务方便，企业也可以通过改变订购的套餐来拓展或者减少模块，服务选择十分灵活。

**其中，公司的核心产品 Falcon 平台是基于两个紧密结合的自有技术：**

（1） **易于部署的轻量级代理。**如今，大部分设备普遍处理能力和计算能力较弱，重量级的代理会降低设备的效率。轻量级的代理可以解决这个痛点，也是公司的核心竞争优势。Falcon 采用非侵入性的部署方式，即时终端用户下线也可以对信息安全进行持续性的保护。此外，轻量级代理的功能高度集成，可以在为顾客提供适应多种场景的解决方案的同时，保证终端运行效率。

（2） **基于云的动态图形数据库：**Threat Graph。受益于众包以及规模效应，大数据提高了 Crowdstrike AI 算法的效率和准确度。同时，公司还使用智能筛选器来处理数据，极大地减少了干扰数据，进一步提升算法效率。

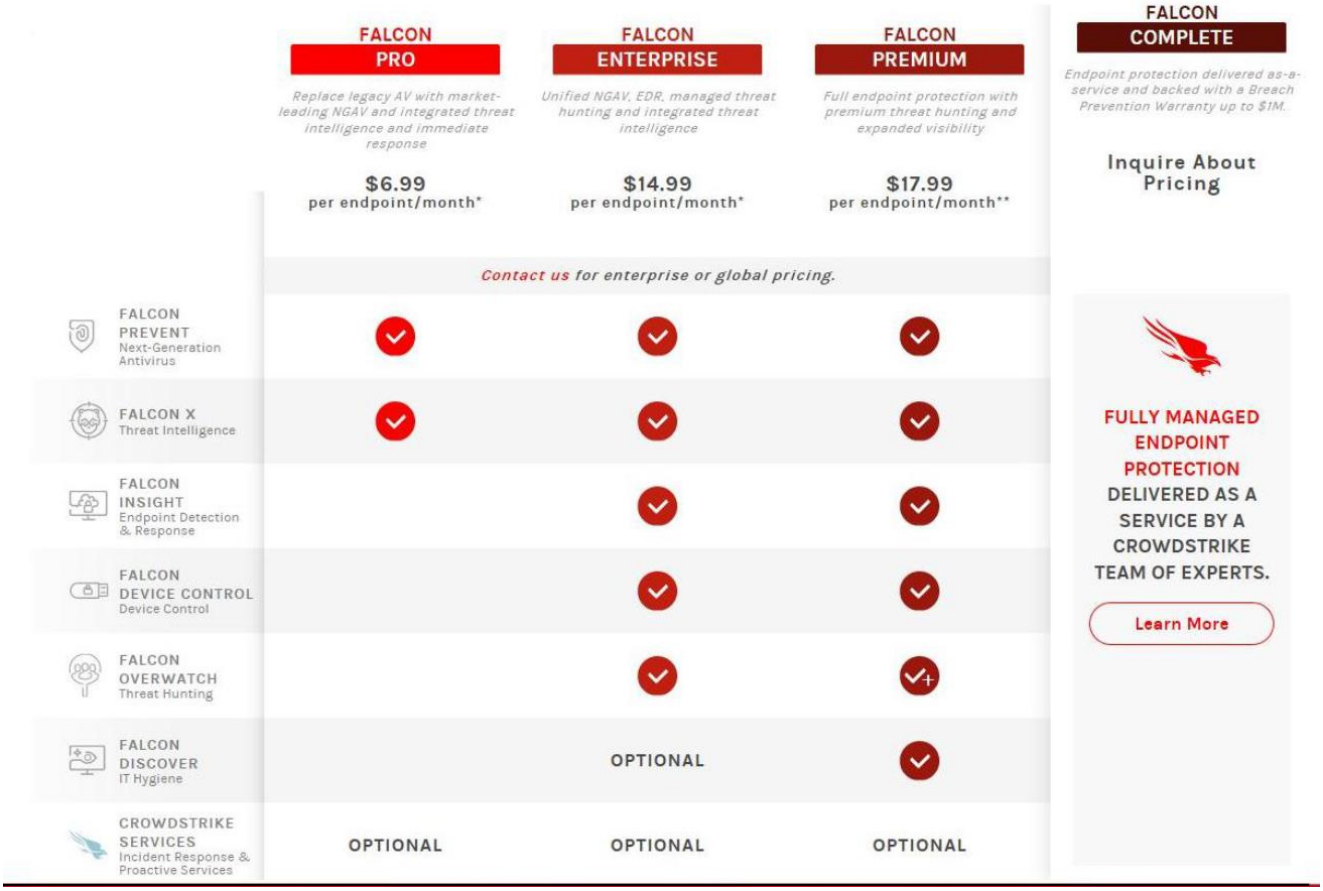
如今，通过 SaaS 订阅的方式，公司在 Falcon 平台为顾客提供 10 种安全模块，覆盖包括终端安全、IT 运维、情报威胁等多个领域。

图表 50：Crowdstrike 产品线结构图


资料来源：公司官网，国盛证券研究所

**部署于云端的平台分析所有订阅用户数据，加速产品迭代与升级，提高客户粘性。**公司的图形数据库可以分析来自所有已订阅的用户的网络安全数据，大量的数据可以帮助算法更好的训练人工智能，从而更好的识别和发现网络安全隐患和事故。这不仅帮助公司更好得保留了现有客户，优秀的算法和保护能力更是吸引了更多新的客户，新的顾客又会产生新的数据，从而不断的完善图形数据库。

图表 51：Crowdstrike 产品收费

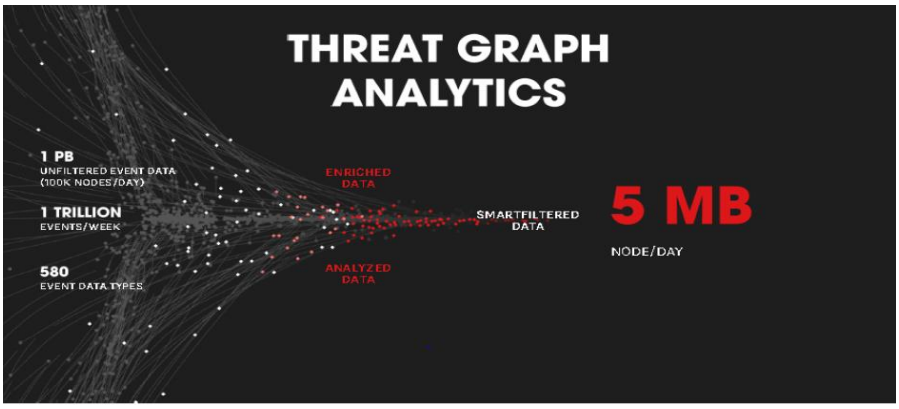



资料来源：公司官网、国盛证券研究所

**轻量级的代理显著地降低了终端设备的计算负担。**根据摩根大通的计算，传统的杀毒软件的 CPU 使用率大约在 13%-30%，而 Crowdstrike 的代理大小为 24MB，CPU 使用率仅占 7%。代理的低 CPU 占有率带来了终端更快的运行。通俗的来说，就是电脑运行的较快，客户使用起来会比较舒心。

**不断完善的图形数据库，智能过滤提升了 Crowdstrike AI 算法的有效性。**本地代理通过对终端产生的数据进行分析，只保留高保真的事件数据并发送至云端，显著地减少了代理的网络负担。高保真的数据被用于训练 AI，使其更能高效准确识别威胁。

*图表 52：智能算法减小网络负担*




*资料来源：公司官网、国盛证券研究所*

## 盈利预测与估值

**收入预测假设：**1）对于网络信息安全基础产品，由于公司的龙头地位，竞争格局较为稳定，收入增速与行业增速差距不大，在 2020-2022 年收入增速分别达到 25%、26%、23%，毛利率较为稳定；2）网络安全信息安全平台在网信办、网安以及大数据局等多个部门对于态势感知平台和大数据智能平台的需求采购，以及云安全的快速增长，在 2020-2022 年收入增速分别达到 70%、55%、48%；3）网络信息安全服务作为政企云安全、大型会议等行业的趋势，未来三年保持快速增长，在 2020-2022 年收入增速分别达到 80%、75%、70%。

图表 53：公司收入拆分及预测

| （单位：亿元） | 2016 | 2017 | 2018 | 2019 | 2020E | 2021E | 2022E |
|---|---|---|---|---|---|---|---|
| **网络信息安全基础产品** | | | | | | | |
| 收入 | 2.08 | 2.70 | 2.97 | 3.84 | 4.72 | 5.67 | 6.80 |
| 增速 | | *30.00%* | *10.00%* | *29.00%* | *23.00%* | *20.00%* | *20.00%* |
| 占比 | *66.17%* | *63.60%* | *48.07%* | *40.68%* | *32.86%* | *26.41%* | *21.33%* |
| 成本 | 0.59 | 0.74 | 0.72 | 0.93 | 1.08 | 1.22 | 1.39 |
| 毛利润 | 1.49 | 1.96 | 2.25 | 2.91 | 3.64 | 4.45 | 5.41 |
| 毛利率 | *71.56%* | *72.46%* | *75.76%* | *75.76%* | *75.76%* | *75.76%* | *75.76%* |
| **网络信息安全平台** | | | | | | | |
| 收入 | 0.18 | 0.51 | 1.42 | 2.72 | 4.49 | 6.97 | 10.31 |
| 增速 | | *184.00%* | *179.00%* | *91.00%* | *70.00%* | *55.00%* | *48.00%* |
| 占比 | *5.70%* | *11.98%* | *22.98%* | *28.78%* | *32.06%* | *33.20%* | *32.99%* |
| 成本 | 0.05 | 0.15 | 0.37 | 0.73 | 1.17 | 1.82 | 2.69 |
| 毛利润 | 0.13 | 0.36 | 1.05 | 1.98 | 3.32 | 5.15 | 7.62 |
| 毛利率 | *74.01%* | *70.45%* | *73.88%* | *72.98%* | *73.88%* | *73.88%* | *73.88%* |
| **网络信息安全服务** | | | | | | | |
| 收入 | 0.67 | 0.92 | 1.63 | 2.64 | 4.75 | 8.32 | 14.14 |
| 增速 | | *36.00%* | *78.00%* | *62.00%* | *80.00%* | *75.00%* | *70.00%* |
| 占比 | *21.43%* | *21.60%* | *26.35%* | *27.97%* | *33.07%* | *38.76%* | *44.35%* |
| 成本 | 0.22 | 0.35 | 0.56 | 0.92 | 1.67 | 2.94 | 5.05 |
| 毛利润 | 0.45 | 0.56 | 1.07 | 1.72 | 3.08 | 5.38 | 9.09 |
| 毛利率 | *67.00%* | *61.50%* | *65.69%* | *64.99%* | 64.87% | 64.63% | 64.27% |
| **第三方硬件产品** | | | | | | | |
| 收入 | 0.21 | 0.12 | 0.16 | 0.24 | 0.28 | 0.32 | 0.35 |
| 增速 | | *-43.00%* | *35.00%* | *51.00%* | *15.00%* | *13.00%* | *10.00%* |
| 占比 | *6.70%* | *2.82%* | *2.61%* | *2.57%* | *2.02%* | *1.60%* | *1.26%* |
| 成本 | 0.18 | 0.11 | 0.15 | 0.22 | 0.26 | 0.29 | 0.32 |
| 毛利润 | 0.03 | 0.00 | 0.01 | 0.02 | 0.02 | 0.02 | 0.03 |
| 毛利率 | *14.06%* | *4.04%* | *7.51%* | *7.51%* | *7.51%* | *7.51%* | *7.51%* |
| **合计** | | | | | | | |
| 收入 | 3.15 | 4.25 | 6.19 | 9.44 | 14.37 | 21.46 | 31.88 |
| 增速 | | *35.00%* | *46.00%* | *52.61%* | *52.26%* | *49.30%* | *48.57%* |
| 成本 | 1.04 | 1.36 | 1.80 | 2.81 | 4.33 | 6.59 | 9.99 |
| 毛利润 | 2.10 | 2.89 | 4.39 | 6.63 | 10.05 | 14.87 | 21.90 |
| 毛利率 | *66.87%* | *67.93%* | *70.90%* | *70.19%* | *69.91%* | *69.27%* | *68.68%* |

资料来源：wind，国盛证券研究所

**费用预测假设：**1）公司在政企端的直销渠道以及中小企业的分销渠道仍在投入期，销售费用持续增长，在 2020-2022 年销售费用增速分别达到 35%、30%、12%；2）公司

研发持续投入，保持技术领先优势，在 2020-2022 年研发费用增速分别达到 45%、40%、35%；3）公司管理费用增速较为平稳，在 2020-2022 年管理费用增速分别达到 28%、25%、20%。

*图表 54：公司费用预测*

| （单位：亿元） | 2016 | 2017 | 2018 | 2019 | 2020E | 2021E | 2022E |
|---|---|---|---|---|---|---|---|
| 销售费用 | 0.92 | 1.29 | 2.06 | 3.16 | 4.27 | 5.55 | 6.93 |
| *增速（%）* | | *40.22%* | *59.69%* | *53.40%* | *35.00%* | *30.00%* | *25.00%* |
| *费用率（%）* | *29.23%* | *30.35%* | *33.30%* | *33.47%* | *30.93%* | *28.32%* | *26.10%* |
| 管理费用 | 0.81 | 0.50 | 0.59 | 0.85 | 1.09 | 1.36 | 1.63 |
| *增速（%）* | | *-38.27%* | *18.00%* | *44.07%* | *28.00%* | *25.00%* | *20.00%* |
| *费用率（%）* | *25.73%* | *11.76%* | *9.54%* | *9.00%* | *7.89%* | *6.95%* | *6.14%* |
| 研发费用 | 0.66 | 0.96 | 1.52 | 2.05 | 2.97 | 4.16 | 5.62 |
| *增速（%）* | | *45.45%* | *58.33%* | *34.87%* | *45.00%* | *40.00%* | *35.00%* |
| *费用率（%）* | *20.97%* | *22.58%* | *24.57%* | *21.72%* | *21.55%* | *21.25%* | *21.15%* |

*资料来源：wind，国盛证券研究所*

**给予“买入”评级。**预计公司 2020-2022 年收入分别为 14.37/21.46/31.88 亿元，增速分别为 52.26%、49.30%、48.57%；利润分别为 1.69/3.14/6.19 亿元，增速分别为 83.54%、85.59%、97.02%，对标美国 CrowdStrike，**给予“买入”评级。**

*图表 55：可比公司估值*

| | | | | EPS | | | PE | | |
|---|---|---|---|---|---|---|---|---|---|
| 证券代码 | 证券简称 | 收盘价（元/股） | 市值（亿元） | 2020E | 2021E | 2022E | 2020E | 2021E | 2022E |
| 688023.SH | 安恒信息 | 323.79 | 239.84 | 1.99 | 3.47 | 6.53 | 162.35 | 93.28 | 49.56 |
| 002439.SZ | 启明星辰 | 47.19 | 440.56 | 0.95 | 1.21 | 1.21 | 49.67 | 38.86 | 38.86 |
| 002065.SZ | 绿盟科技 | 14.45 | 450.19 | 0.36 | 0.45 | 0.45 | 40.58 | 32.15 | 32.15 |
| 300454.SZ | 深信服 | 238.02 | 973.67 | 2.23 | 3.03 | 3.03 | 106.57 | 78.55 | 78.55 |
| 300352.SZ | 北信源 | 8.45 | 122.51 | 0.14 | 0.20 | 0.20 | 61.95 | 43.07 | 43.07 |
| 002212.SZ | 南洋科技 | 29.61 | 343.03 | 0.54 | 0.75 | 0.75 | 54.51 | 39.43 | 39.43 |
| 002268.SZ | 卫士通 | 24.61 | 206.31 | 0.32 | 0.44 | 0.44 | 77.17 | 55.42 | 55.42 |

*资料来源：wind，国盛证券研究所*

## 风险提示

**行业竞争加剧：**随着云安全、工控安全等安全领域的强势增长，安全厂商纷纷拓张新市场，在激烈的竞争中，公司有可能占不到较大的市场份额。
**公司安全服务与平台增速推进不及预期：**公司安全服务与平台业务订单增长不及预期。
**关键假设可能存在误差的风险：**部分关键假设存在产业逻辑分析，与未来发生的实际情况可能存在偏差。

## 免责声明

国盛证券有限责任公司（以下简称"本公司"）具有中国证监会许可的证券投资咨询业务资格。本报告仅供本公司的客户使用。本公司不会因接收人收到本报告而视其为客户。在任何情况下，本公司不对任何人因使用本报告中的任何内容所引致的任何损失负任何责任。

本报告的信息均来源于本公司认为可信的公开资料，但本公司及其研究人员对该等信息的准确性及完整性不作任何保证。本报告中的资料、意见及预测仅反映本公司于发布本报告当日的判断，可能会随时调整。在不同时期，本公司可发出与本报告所载资料、意见及推测不一致的报告。本公司不保证本报告所含信息及资料保持在最新状态，对本报告所含信息可在不发出通知的情形下做出修改，投资者应当自行关注相应的更新或修改。

本公司力求报告内容客观、公正，但本报告所载的资料、工具、意见、信息及推测只提供给客户作参考之用，不构成任何投资、法律、会计或税务的最终操作建议,本公司不就报告中的内容对最终操作建议做出任何担保。本报告中所指的投资及服务可能不适合个别客户，不构成客户私人咨询建议。投资者应当充分考虑自身特定状况，并完整理解和使用本报告内容，不应视本报告为做出投资决策的唯一因素。

投资者应注意，在法律许可的情况下，本公司及其本公司的关联机构可能会持有本报告中涉及的公司所发行的证券并进行交易，也可能为这些公司正在提供或争取提供投资银行、财务顾问和金融产品等各种金融服务。



## 分析师声明

本报告署名分析师在此声明：我们具有中国证券业协会授予的证券投资咨询执业资格或相当的专业胜任能力，本报告所表述的任何观点均精准地反映了我们对标的证券和发行人的个人看法，结论不受任何第三方的授意或影响。我们所得报酬的任何部分无论是在过去、现在及将来均不会与本报告中的具体投资建议或观点有直接或间接联系。

## 投资评级说明

| 投资建议的评级标准 | | 评级 | 说明 |
|---|---|---|---|
| 评级标准为报告发布日后的 6 个月内公司股价（或行业指数）相对同期基准指数的相对市场表现。其中 A 股市场以沪深 300 指数为基准；新三板市场以三板成指（针对协议转让标的）或三板做市指数（针对做市转让标的）为基准；香港市场以摩根士丹利中国指数为基准，美股市场以标普 500 指数或纳斯达克综合指数为基准。 | 股票评级 | 买入 | 相对同期基准指数涨幅在 15%以上 |
| | | 增持 | 相对同期基准指数涨幅在 5%~15%之间 |
| | | 持有 | 相对同期基准指数涨幅在-5%~+5%之间 |
| | | 减持 | 相对同期基准指数跌幅在 5%以上 |
| | 行业评级 | 增持 | 相对同期基准指数涨幅在 10%以上 |
| | | 中性 | 相对同期基准指数涨幅在-10%~+10%之间 |
| | | 减持 | 相对同期基准指数跌幅在 10%以上 |

**国盛证券研究所**

**北京**
地址：北京市西城区平安里西大街 26 号楼 3 层
邮编：100032
传真：010-57671718
邮箱：gsresearch@gszq.com

**上海**
地址：上海市浦明路 868 号保利 One56　1 号楼 10 层
邮编：200120
电话：021-38934111
邮箱：gsresearch@gszq.com

**南昌**
地址：南昌市红谷滩新区凤凰中大道 1115 号北京银行大厦
邮编：330038
传真：0791-86281485
邮箱：gsresearch@gszq.com

**深圳**
地址：深圳市福田区福华三路 100 号鼎和大厦 24 楼
邮编：518033
邮箱：gsresearch@gszq.com