中国银河证券|CGS

# 信息安全的边界与未来

## CHINA GALAXY SECURITIES CO., LTD.

**分析师**
**钱劲宇**
执业证书编号：S0130517110002

特别鸣谢
李璐昕
对此报告的编制提供信息

**中国银河证券股份有限公司**
**CHINA GALAXY SECURITIES CO., LTD.**

# 报告摘要

**1. 信息安全边界在不断扩展，提振需求量。**
- 数字化转型发展推动网络安全问题加剧，攻击的数量、多样性以及损害的程度大幅提升。
- 新兴技术如云计算和物联网等推动保护对象进一步拓展。
- 政策的发展与逐步完善对企业提出更高要求。

**2. 国内外厂商安全产品一体化趋势显著，云安全和端点防护是未来趋势所在。**
- 国内外厂商寻求将端点保护、威胁防护、云安全、SIEM以及云端威胁情报等整合在同一应用框架内，产品趋向于平台化供应。
- 一体化平台具有整合效应，促使厂商大额订单数量激增，行业头部效应初显。
- 端点防护和云平台是各大厂商近年布局重点。
- 搭载AI的云平台萌发。

**3. 国内外网络安全空间广阔，增速稳健，国内厂商仍有上升空间。**
- 对比国内外GDP、IT支出、IT网络安全支出状况，中国网安市场空间望不断释放。
- 国内政策发展落地加速，等保2.0利好规模提升。
- 国内领先厂商无论在收入、利润还是研发水平上均与全球领先厂商具有一定差距。

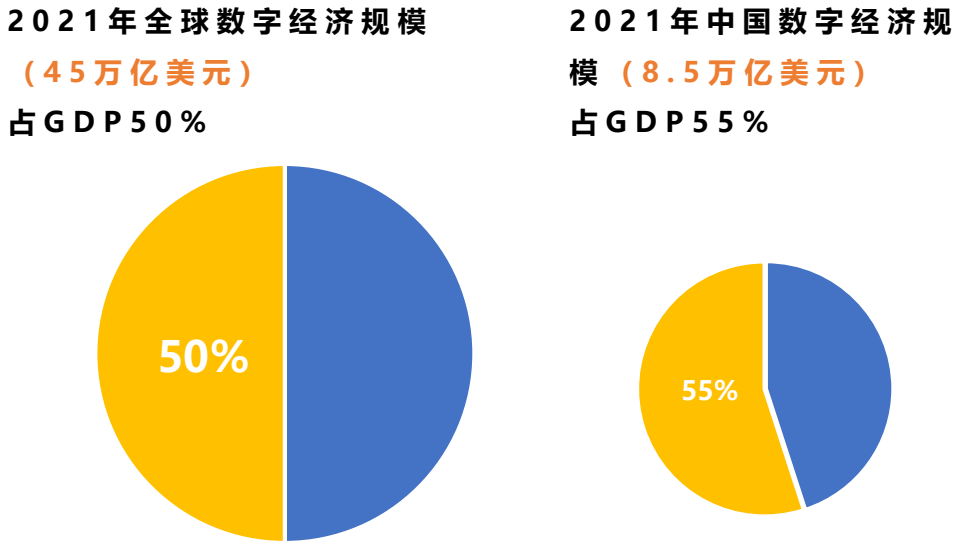
# 目 录

# 1.1 网络安全边界扩展，推动更多需求

## 1.1.1 数字化转型加快，网络安全形势严峻

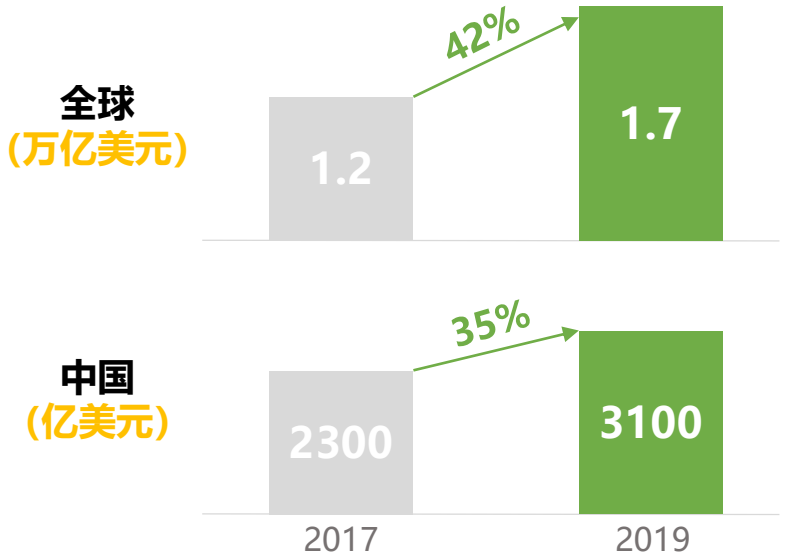
IDC预测，2021年全球数字经济将占整体GDP50%，中国为55%。预计全球数字化转型相关ICT （Information and Communication Technology）支出2019年达到1.7万亿美元，中国约3100亿美元。到2020年，全球整体ICT支出大约为4到5万亿美金，其中30%到40%左右都跟数字化转型相关。企业数字化进程带来网络安全问题加剧，网络安全犯罪引发的经济损失日益增多。

图1 全球&中国数字经济规模预测




来源：IDC，中国银河证券研究院整理

图2 全球&中国数字化转型相关ICT支出



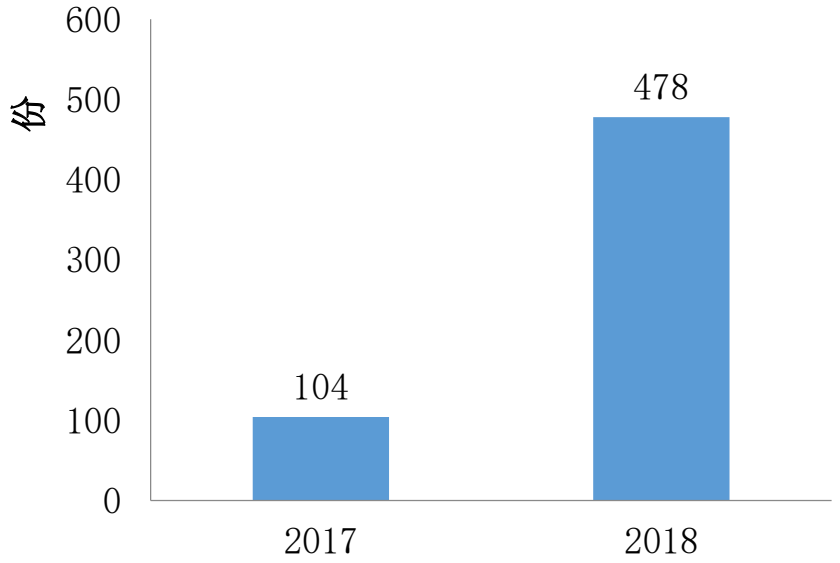

来源：IDC，中国银河证券研究院整理

## 1.1.2 全球网络安全威胁增加

根据Symantec《互联网安全威胁报告》，全球面临的APT攻击、移动设备威胁、IoT威胁增加：APT攻击手段多样化，全球高级持续性威胁相关公开报告从2017年的104份增加到2018年的478份；移动恶意软件感染总数在2018年有所下降，但勒索软件感染数量与2017年相比却迅速增加了三分之一；IoT攻击数量在2017年大幅增加后，在2018年趋于稳定，2018年针对赛门铁克物联网诱捕系统的攻击月均达到5200次。

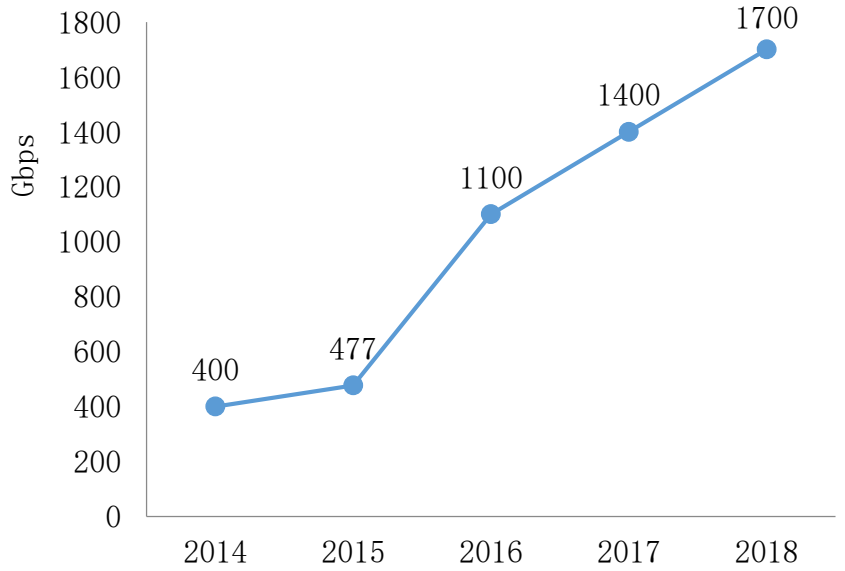
根据华为《2018年全球DDoS攻击现状与趋势分析》，攻击的低成本、平台化和服务化及行业内激烈竞争促使攻击流量峰值、攻击频率不断提升，最近5年全球DDoS攻击最大攻击流量峰值持续增长。

图3 2017-2018年全球高级持续性威胁（APT）相关公开报告




来源：Symantec，中国银河证券研究院整理

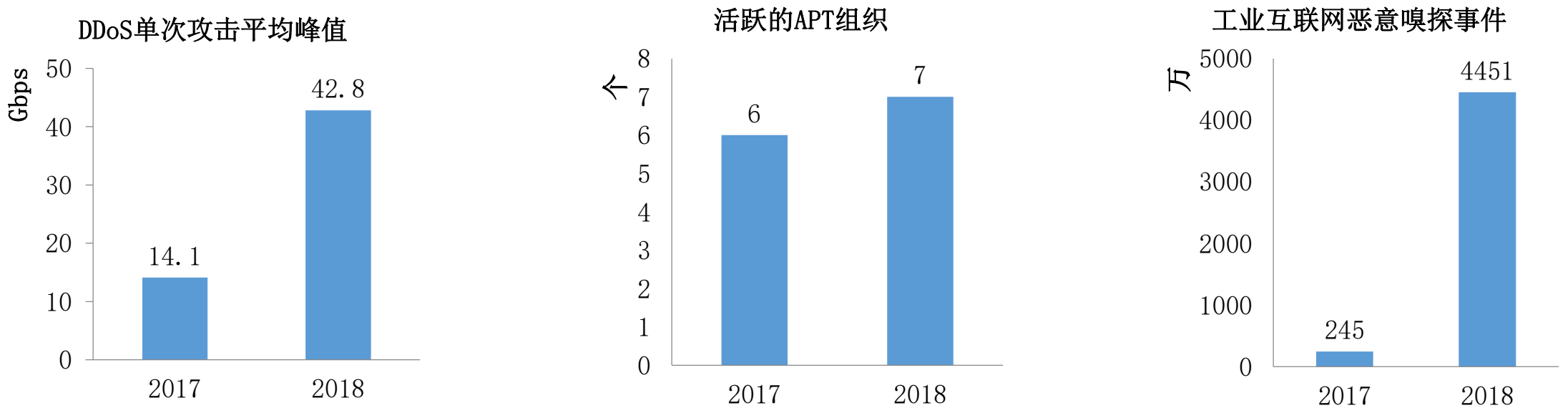
图4 最近5年全球DDoS攻击最大攻击流量峰值




来源：华为，中国银河证券研究院整理

2018年我国发生多起如勒索病毒的大规模网络危害事件，关键信息基础设施面临的安全风险值得关注，APT攻击、DDoS攻击等问题也较为严重。与2017年相比，DDoS单次攻击平均峰值增加了2倍有余，主要原因是网络带宽的普遍提高和攻击者掌控的DDoS攻击能力有了大幅的提升；活跃的APT组织数新增一个；工业互联网恶意嗅探事件暴增约17倍，针对工业控制系统的定向性攻击趋势明显。

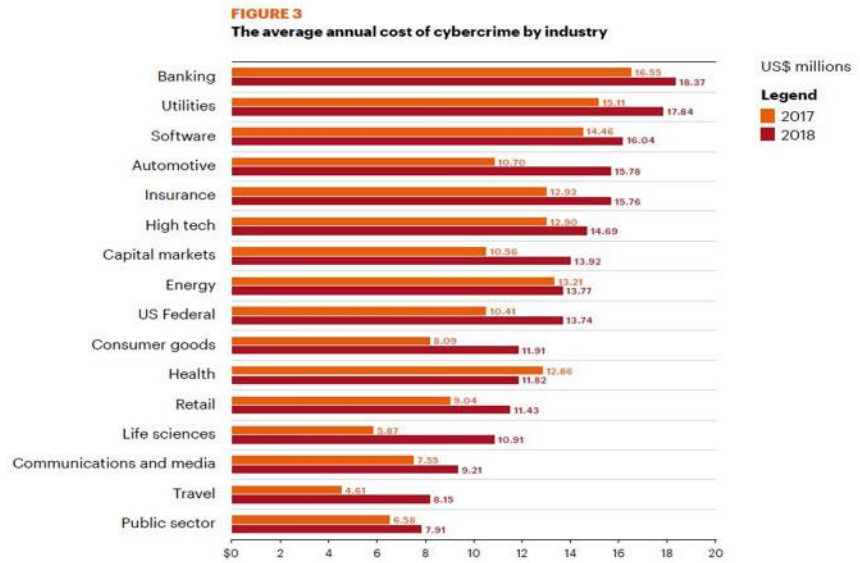
图5 2017-2018年中国网络攻击态势对比




*来源：国家计算机网络应急技术处理协调中心，绿盟，360威胁情报中心，中国银河证券研究院整理*

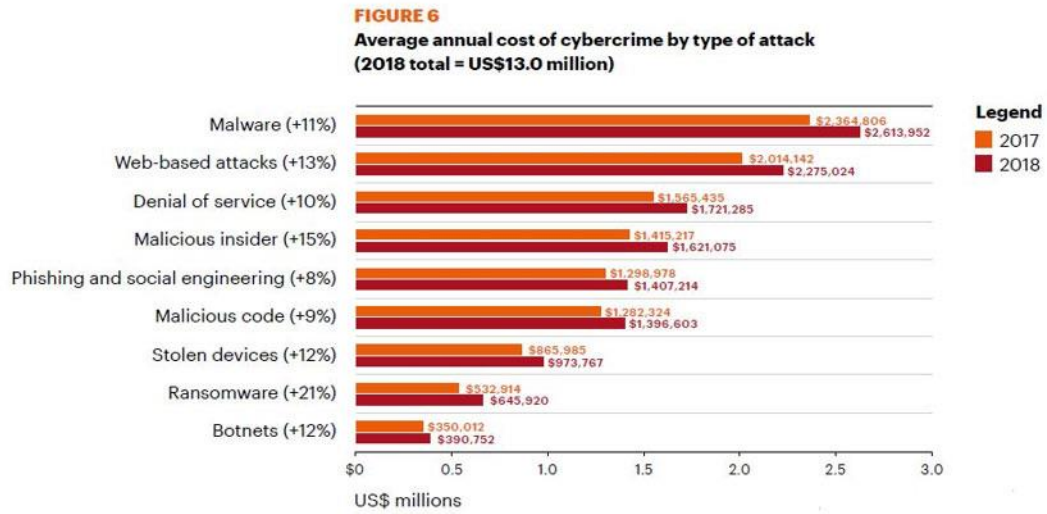
2019年3月，埃森哲联合Ponemon针对11个国家16个行业的355家大型公司发布了第九次网络犯罪成本调研报告。报告说明，企业组织应付网络攻击犯罪的成本随着日益多元化的网络入侵方式而不断上升，预计从2019年到2023年总的网络安全成本在5.2万亿美元，同时网络犯罪为这355家企业带来的平均成本在2018年达到了1300万美元，同比2017年增长了12%。其中网络犯罪给银行业带来的成本（损失）相对最大，对旅游业和政府公共部门带来的影响较小；恶意软件对大型企业造成的损失高达2600千万美元，勒索软件带来的网络安全损失增长位居首位。

图6 2017-2018年分行业网络安全成本




来源：埃森哲，中国银河证券研究院整理

图7 2017-2018年分类别网络犯罪造成损失




来源：埃森哲，中国银河证券研究院整理

进一步对各个网络犯罪方式带来的损失进行细分分析，Dos攻击对企业工作终止造成的损失最大，恶意软件、web攻击和恶意代码带来的损失主要是关于信息泄露方向，同时信息泄露也是所有损失类型中占比最多的组别。

从企业组织为了对抗网络安全威胁所投入成本的不同阶段来看，最大部分的成本（36%）花费在了发现攻击这一阶段中，遏制攻击的成本近四年平均占比最小但却在逐年上升中，恢复攻击造成损失的花费下降迅速（18%），我们认为这与企业越来越重视网络安全，做好重要数据的预案备份有关。

图8 2018年网络犯罪造成损失分类

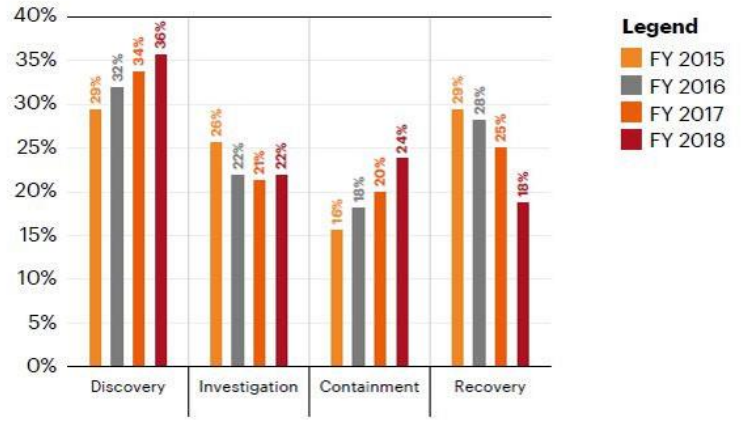
FIGURE 8
**Consequences of different types of cyberattacks**
**(average annual cost; figures in US$ million; 2018 total = US$13.0 million)**

| | Business disruption | Information loss | Revenue loss | Equipment damage | Total cost by attack type |
|---|---|---|---|---|---|
| Malware (+11%) | $ 0.5 | $ 1.4 | $ 0.6 | $ 0.1 | $ 2.6 |
| Web-based attacks (+17%) | $ 0.3 | $ 1.4 | $ 0.6 | $ – | $ 2.3 |
| Denial-of-service (+10%) | $ 1.1 | $ 0.2 | $ 0.4 | $ 0.1 | $ 1.7 |
| Malicious insiders (+15%) | $ 0.6 | $ 0.6 | $ 0.3 | $ 0.1 | $ 1.6 |
| Phishing and social engineering (+8%) | $ 0.4 | $ 0.7 | $ 0.3 | $ – | $ 1.4 |
| Malicious code (+9%) | $ 0.2 | $ 0.9 | $ 0.2 | $ – | $ 1.4 |
| Stolen devices (+12%) | $ 0.4 | $ 0.4 | $ 0.1 | $ 0.1 | $ 1.0 |
| Ransomware (+21%) | $ 0.2 | $ 0.3 | $ 0.1 | $ 0.1 | $ 0.7 |
| Botnets (+12%) | $ 0.1 | $ 0.2 | $ 0.1 | $ – | $ 0.4 |
| **Total cost by consequence** | $ 4.0 | $ 5.9 | $ 2.6 | $ 0.5 | **$ 13.0** |

*来源：埃森哲，中国银河证券研究院整理*

图9 网络安全防护各阶段成本

FIGURE 9
**Percentage of expenditure by internal activity**

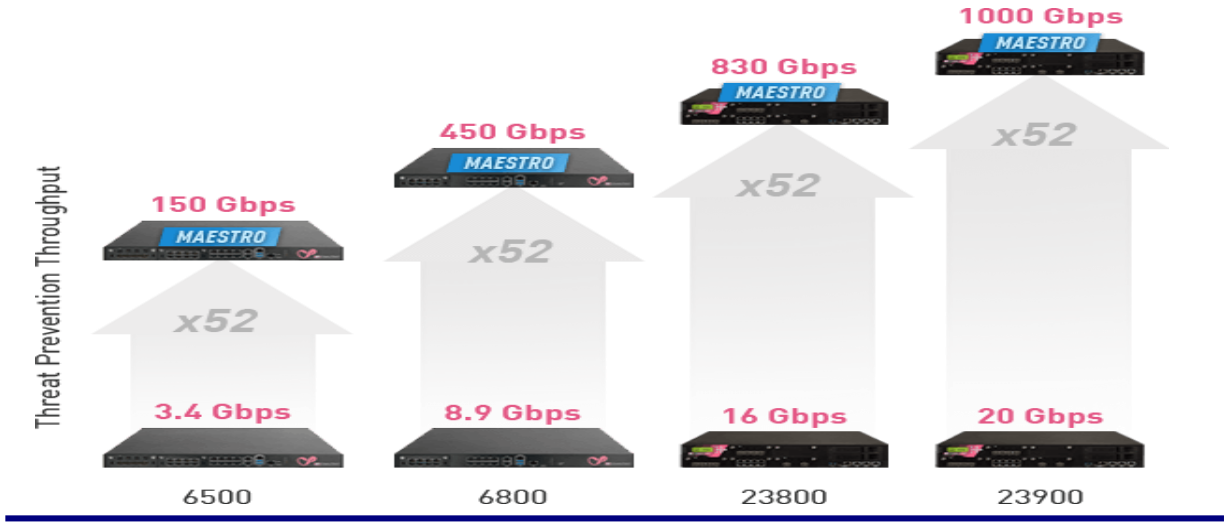



*来源：埃森哲，中国银河证券研究院整理*

## 1.1.3 保护对象的增多

随着物联网、车联网和5G的技术的不断应用，网络安全的边界也在不断扩张，网络安全厂商在传统端点防护的基础上加入对**IoT以及移动设备**，以及对**5G设备、车联网**的支持，以应对新的僵尸网络威胁， 例如在5G方面，Check Point针对5G存在的数据流量跨升推出的Maestro架构，将防火墙单个网关扩张至原来的50倍大小，可以允许极大规模流量传输。在车联网方面，Fortinet也与瑞萨电子合作互联汽车网络安全方案，该产品整合了飞塔的FortiOS安全操作系统及瑞萨电子R-Car H3系统晶片；2016年赛门铁克发布了汽车异常行为探测解决方案。

图10 Maestro架构




*来源：公司官网，中国银河证券研究院整理*

# 1.2 政策与事件催生安全需求



面对不断增加的全球网络安全威胁，许多国家在九十年代初就把信息化作为国策，重视信息安全工作并出台了一系列重要政策、措施，进一步推动了企业的安全需求。

图11 网络安全发展史

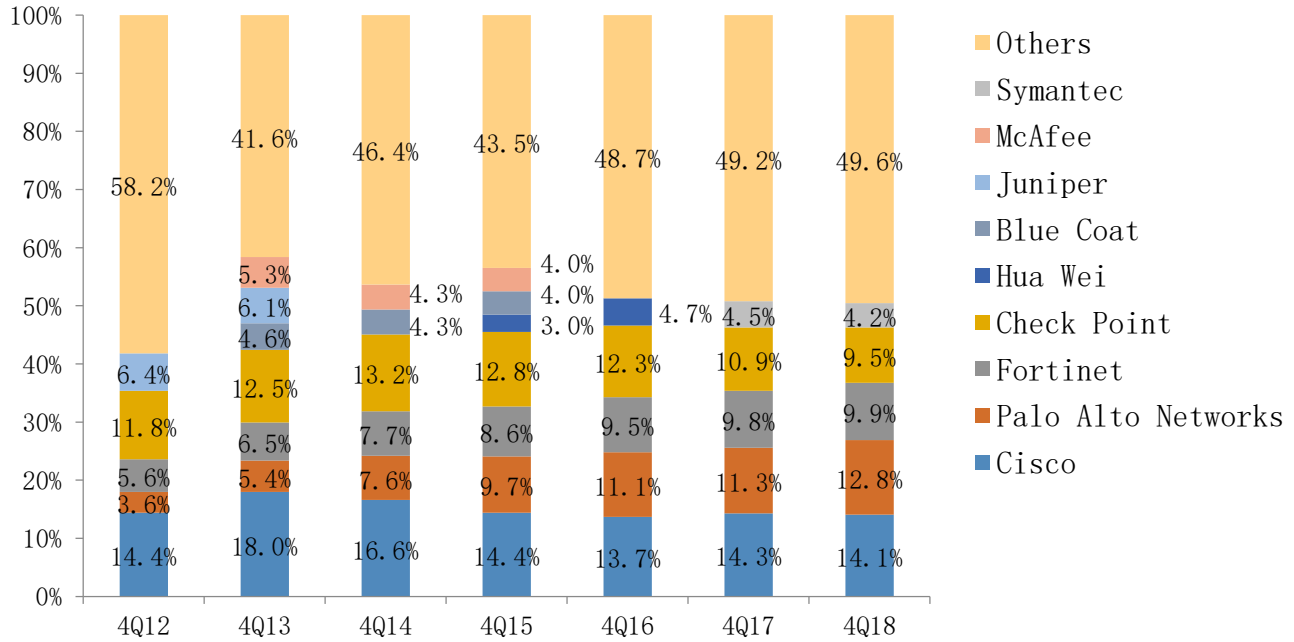
| 时间 | 网络安全发展史 |
| --- | --- |
| 1986年 | 莫里斯蠕虫病毒等第一批互联网病毒肆虐，引发对网络安全的关注。 |
| 1987年 | 第一个专门安全机构——国家信息中心信息安全处成立，中国计算机安全事业开始探索，尚无相关法律法规完整规章，主要内容是实体安全。 |
| 80年代末 | 第一代网络防火墙出现，依附于路由器的包过滤功能，后逐渐发展为独立专用的设备。 |
| 90年代初 | 世界信息技术革命使许多国家把信息化作为国策，信息化进程带动网络安全进入快速发展期。 |
| 1994年 | 公安部颁布了《中华人民共和国计算机信息系统安全保护条例》，这是我国第一个计算机安全方面的法律，标志安全产业正式起步。<br>第一代“状态”防火墙出现，Check Point开创“状态监视”一词。 |
| 1999年 | 国家计算机网络与信息安全管理协调小组成立，国家信息安全走向正轨。 |
| 21世纪初 | 美国国家安全局和美国国防部相继颁布信息保障技术框架（IATF）及信息保障的实施的命令8500.2，进入整体角度考虑的信息安全保障时代。 |
| 2007年 | 《信息安全等级保护管理办法》出台，明确了信息安全等级保护制度的基本内容，标志着等保1.0的落地。<br>Palo Alto Networks推出第一个自主研发的防火墙，符合两年后Gartner发布的“下一代防火墙”特性。 |
| 2016年 | 11月表决通过了《中华人民共和国网络安全法》，是网络空间法制化的里程碑成果。 |
| 2018年 | Gartner报告称，企业级网络防火墙市场相对成熟稳定，与2017魔力象限相比，没有新入者，也没有出局者。 |
| 2019年 | 5月13日《信息安全技术网络安全等级保护基本要求》正式发布，标志着等级保护标准正式进入2.0时代。 |

*来源：安全部，公司官网，中国银河证券研究院整理*

# 1.3 网络安全边界拓展，功能增多

经过多年的发展，根据IDC数据，在**安全设备市占率**方面，Cisco、Palo Alto Networks、Fortinet、Check Point和Symantec五家企业位居前列，除去公司业务较为广泛的Cisco，四家总和接近市场的40%。

图12 Worldwide Top 5 Security Appliance Companies, 2018Q4 Vendor Revenue Market Share




*来源：IDC，中国银河证券研究院整理*

# 1.3.1 下一代防火墙

下一代防火墙（NGFW）是网络安全服务的核心支柱，其对云安全、端点防护和云端威胁情报分析的一体化整合，结合机器学习、人工智能优化防护能力，具备软件即服务(SaaS)应用模式，能为用户提供有效的应用层一体化安全防护，帮助用户安全地开展业务并简化用户的网络安全架构。根据Gartner魔力象限报告，Palo Alto Networks和Check point已经连续数年占据**领导者象限**，Fortinet近两年也位列**领导者象限**。因此，选取这三家行业领导者与老牌网络安全公司Symantec作为国外网络安全厂商的代表。

图13 Gartner企业级网络防火墙魔力象限（2018年）


*来源：Gartner，中国银河证券研究院整理*

在下一代防火墙领域，国外网络安全厂商均早在数年前推出了NGFW的相关产品，其中Palo Alto Networks是最先定义并上市NGFW的领军企业，并于近期增加了其关于SaaS服务的支持。

图14 网络安全企业NGFW代表产品

| 公司 | Fortinet | Check Point | Palo Alto Networks | 深信服 | 山石网科 | 华为 |
|---|---|---|---|---|---|---|
| 下一代防火墙产品 | FortiGate | Check Point Security Gateway Series | PA Series | 深信服AF | SG-6000系列 | 华为防火墙 |
| 优点 | -相较其他安全厂商产品性价比较高 | --所有产品具有统一的软件刀片架构（blade）<br>--拥有最大的威胁检测团队；更重视垂直行业需要的细分安全方案 | --以防火墙为平台，提供丰富的安全订阅服务；业内率先推出防火墙即服务<br>--单通道平行处理架构 | -可视化强，操作简便 | --Cloudhive和Cloudedge产品能够适用于企业的混合多云<br>--CloudEdge对国内外主流公有云平台都支持客户对QOS、异常行为检测、流量分析；能够精准显示攻击的状态 | --专注云安全，应用控制方面较为出色；欧洲、中东、拉丁美洲地区市场开拓较快。生态好、网络设备的客户喜欢被cross-sell<br>--性价比（吞吐量/价格）较高。 |
| 缺点 | -防火墙缺乏高级功能、创新功能被大型企业所诟病 | --同时使用多个广域网连接时性能较差，防火墙在长时间高负荷下，性能持续性不足<br>--只能解密HTTPS，缺少对FTPS和SSH协议支持 | --价格昂贵<br>--中央管理平台Panorama管理过多防火墙时效率变低 | -除阿里云之外，目前未与其他IaaS平台集成方案；不支持双栈环境；沙箱只支持Windows | --UI界面和报告体验不佳；E和T系列的防火墙产品容易被混淆；只限于公有云提供沙箱功能 | -功能更新不够快；GUI的设计不够简便；海外客户的服务响应不够及时。 |

来源：公司官网，中国银河证券研究院整理

## 1.3.2 一体化安全架构

- 网络安全行业战略整体趋势是构建以端点防护、云安全还有威胁防护为核心的一体化防火墙架构和可视化的操作平台，并通过机器学习、人工智能和云智能来优化防护能力。
- 将机器学习、人工智能与云溶于防火墙防护中，本地端和云端联合，威胁信息实时共享，借助机器学习训练本地防火墙防护能力，更好的应对勒索病毒和零日漏洞问题。通过人工智能主动分析文件行为，在破坏发生前发现隐蔽性攻击进行分类和控制，建立可视化的界面和一体化便于管理的平台。
- 在威胁事件的事前利用沙盘模拟可疑事件可能带来的影响、利用**欺骗和诱饵技术**来进行主动式的威胁防护，事中快速响应威胁文件并追根溯源，使用用户**行为分析**(UEBA)识别不同类型的异常用户行为，事后利用**安全信息与事件管理**(SIEM)建立事件库记录、分析，以应对下一次有可能的安全事件。

图15 网络安全企业安全产品集成平台

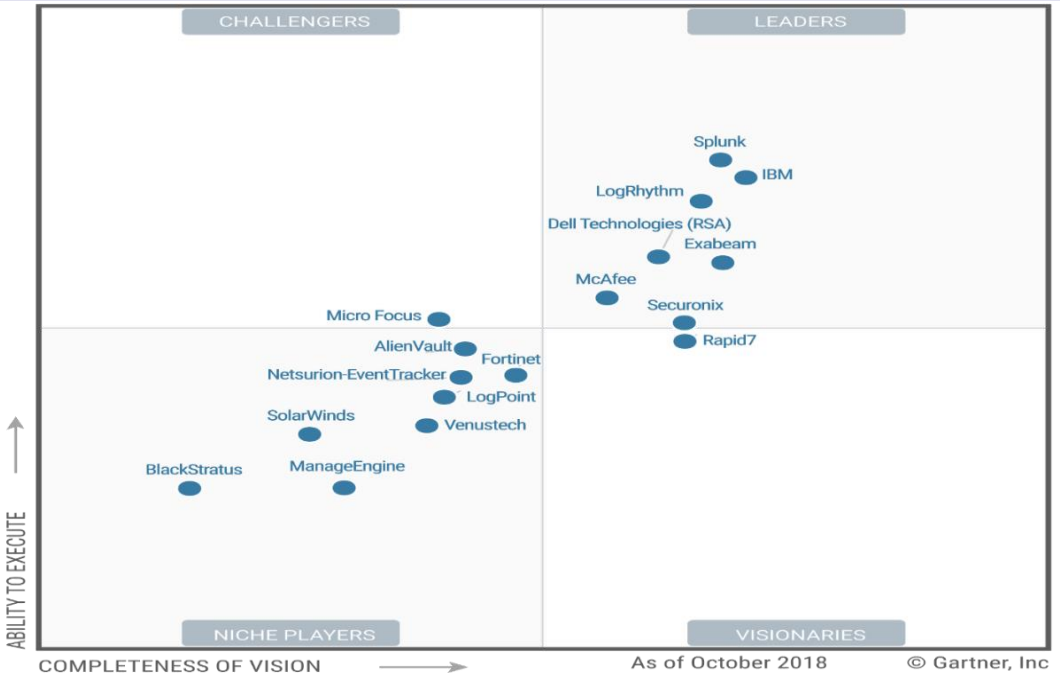
| 公司 | Fortinet | Symantec | Check Point | Palo Alto Networks |
|---|---|---|---|---|
| 全安全防护平台产品 | Fortignet Security Fabric | Integrated Cyber Defense (ICD) | Check Point Infinity | Security Operating Platform |

来源：公司官网，中国银河证券研究院整理

## 1.3.3 SIEM

在传统端点保护的基础上，增进对**端点威胁的响应**（SOAR）以及一体化的**安全事件管理**（SIEM），快速检测威胁、减少安全人工分析投入，提高安全运营的效率。**SIEM**涉及到网络安全的各个领域，根据Gartner魔力象限，SIEM市场存在第一集团三家领军企业IBM、Splunk、LogRhythm，产品战略大多在高级安全分析领域围绕UEBA，在安全响应领域围绕SOAR，同时聚焦于云计算环境下的SIEM应用场景，譬如针对云计算推出支持安全托管服务提供商(MSSP)和SaaS版本的SIEM。

图16 GartnerSIEM魔力象限（2018年）




*来源：Gartner，中国银河证券研究院整理*

# 1.3.4 传统防火墙玩家加码端点防护

在端点防护领域，赛门铁克在Gartner列为领导者象限的地位占据绝对优势。Fortinet与Palo Alto Networks也上榜，作为防火墙领域的王者，Palo Alto Networks的端点防护能力来源于对终端安全公司Cyvera的收购，并不是传统端点防护的玩家，但随着一系列收购对Traps进行功能整合与强化，集成沙箱Wildfire能力，我们看好Palo Alto Traps产品后续的发展

图17 Gartner端点防护魔力象限（2018年）


*来源：Gartner，中国银河证券研究院整理*

在端点防护领域，赛门铁克以六家企业中唯一一家被Gartner列为领导者象限的公司的地位占据绝对优势，传传统企业防火墙厂商在端点防护上均有相对应的布局，战略趋势以整合端点安全、威胁防护和云安全为主。

图18 网络安全厂商端点防护产品

| 公司 | Fortinet | Symantec | Check Point | Palo Alto Networks | 深信服 | 启明星辰 |
|---|---|---|---|---|---|---|
| 端点防护 | FortiClient<br>FortiNAC | Symantec Endpoint Security | Check Point Endpoint Security | Traps Advanced Endpoint Protection | 终端检测响应平台EDR | 云子可信 |
| 特点 | --Forticlient 的单独模块可以与其它安全厂商的安全产品配合使用<br>-恶意软件保护技术欠佳<br>--Forticlient的恶意软件保护引擎是基于规则和签名的，没有Fortinet威胁保护的其他组件，较难检测恶意操作以及零日漏洞。 | --第一个在单一时代将恶意软件保护、EDR、系统强化和欺骗功能结合在一起的供应商。<br>--EDR技术被Gartner列为领导者象限，第三方测试分数保持在第一位<br>--宣传力度欠佳，销售投入有待增长。 | --更重视垂直行业需要的细分安全方案<br>-- 对移动端iOS和Android的防护威胁发现率高于其他公司 | --不依赖签名，尽管它使用WildFire平台通过文件哈希值执行快速查杀，但它能够在脱机时阻止恶意软件/勒索软件<br>--与SoC自动化供应商（如Splunk、ServiceNow和Phantom）有很强的集成 | --智能引擎减少误报，不与底层驱动挂勾的Agent广泛兼容各种操作系统，解决了传统EDR的两大弊端：警报疲劳和兼容性，体现了安全系统的智能化、整体化，协同化。 | --强大的终端安全管理能力、良好的用户体验与可达性和高效的 P2P 客户端升级方式 |

来源：公司官网，中国银河证券研究院整理

## 1.3.5 云安全兴起

针对企业接入公有或私有云过程中的安全隐患，完善云访问安全代理(CASB)防护能力，一方面控制数据流通过程中的泄露问题和潜在合规性隐患，提供API或终端代理，接管用户数据，并对不同职能区域进行微隔离；另一方面建立可视化云安全配置管理(CSPM)，对IaaS，以及PaaS，甚至SaaS的控制平面中的基础设施安全配置进行分析与管理。在云安全领域方面，国外网络安全行业代表性厂商中，无论是在虚拟机安全，还是针对云使用安全（CASB）都有较为完善的布局。

图19 网络安全厂商云安全产品

| 公司 | Fortinet | Symantec | Check Point | Palo Alto Networks |
|---|---|---|---|---|
| 云安全 | Fortinet Fabric Connectors<br>FortiCASB | CloudSOC Cloud Access Security Broker（CASB）<br>Hybrid Cloud Security | Check Point vSEC (CloudGuard)<br>Check Point ThreatCloud | Global Protect Cloud Service<br>VM-Series<br>Aperture(CASB) |
| 特点/弱势 | --完善的云产品布局<br>--对非Windows架构系统兼容性较差，对于Mac无法提供完整云安全服务 | --唯一通过内置集成功能在 CASB 中整合DLP、SWG和端点防护等安全产品的厂商 | --Maestro架构对私有云和公有云统一管理，用户可以在混合架构下可以更加智能、统一的部署安全策略，提高工作效能并降低人为错误 | --能够精准识别第三方SaaS的风险 |

*来源：公司官网，中国银河证券研究院整理*

CASB作为企业使用公有云时，如何管理敏感数据最重要的一环，Gartner认为2022年60%的企业在使用云服务时，都会采用CASB。

图20 Gartner2018年CASB魔力象限

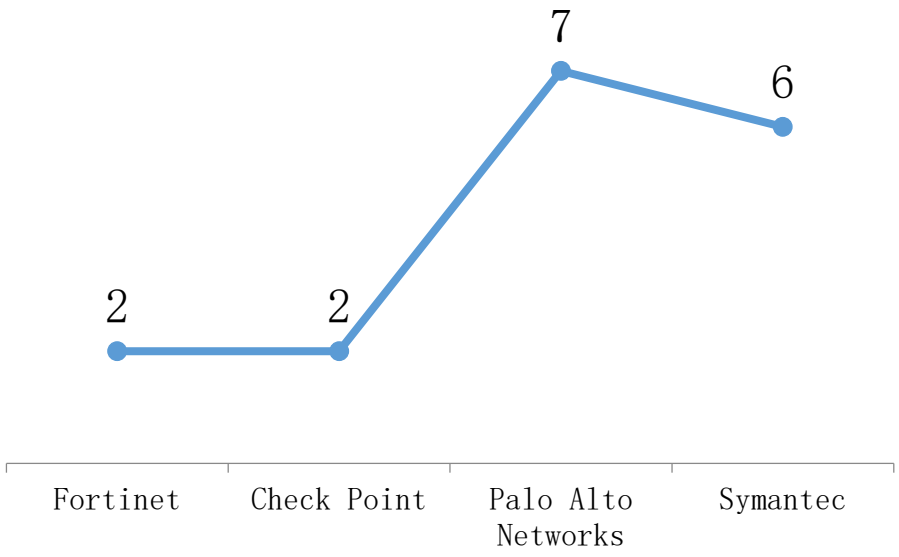

*来源：Gartner，中国银河证券研究院整理*

# 1.4 安全巨头战略方向

## 1.4.1 M&A聚焦

围绕着各个安全领域，2017-2019年间四家公司总计完成了**17**起并购收购事宜，收购最主要方向是云安全，占到整体并购案例的6/17，余下依次分别为**端点防护与响应(EDR)、威胁防护、SIEM**。分技术方向来看，EDR与云智能的结合以及对端点安全概念的延伸（IoT和Mobile）仍然是发展的主要方向，诸如Palo Alto推出的**Cortex XDR**以及赛门铁克更新的**托管型端点检测和响应(MEDR)**服务。同时，云安全尤其是公有云安全也是行业发展的热点，尤其是对**云的安全访问（CASB）、云安全管理的可视化以及微隔离**等等。

图21 2017年起M&A案例数




来源：公司官网，中国银河证券研究院整理

图22 2017年起收购公司技术方向

| M&A方向 | Fortinet | Check Point | Palo Alto Networks | 赛门铁克 |
|---|---|---|---|---|
| Cloud Security | | ○ | ○○○ | ○○ |
| Threat Protection | | | ○ | ○ |
| EDR（包括IoT和Mobile） | ○ | ○ | ○ | ○○ |
| SIEM | ○ | | ○ | |
| 其他 | | WAAP | CWPP | VPN |

来源：公司官网，中国银河证券研究院整理

# 1.4.2 Palo Alto收购与新产品布局

Palo Alto的并购活动为四家公司之冠，并且在刚刚进行的2019 Q2财季的报告上宣布了其即将对专精于容器安全的**Twistlock**和无服务器运算（Serverless）安全业者**PureSec**进行收购，作为网络安全行业的领军企业，预计其安全服务的边界将不断扩张，技术优势将进一步扩大。

图23 2017年起Palo Alto收购案例

| 公司名称 | 日期 | 收购对象 | 技术方向 | 详细说明 |
|---|---|---|---|---|
| Palo Alto Networks | 2017.2.28 | LightCyber | Threat Protection | 使用行为分析和异常检测来检测针对性的攻击，内部威胁 |
| | 2018.3.26 | Evident.io | Public Cloud Security | 识别和评估公有云的安全风险并通过单一管理提高整体的云安全状况。 |
| | 2018.4.24 | Secdo | EDR | 优越的数据收集和可视化方法，增强Palo Alto Networks可视化、快速检测和阻止潜在威胁的能力 |
| | 2018.10.12 | RedLock | Cloud Security | 使用AI扫描企业部署寻找恶意活动，检查云环境安全设置是否符合法规 |
| | 2019.3.28 | Demisto | SOAR | 提供编排和自动化安全技术，即时威胁预防和快速反应的能力 |
| | 2019.5.30 | Twistlock | CWPP | 漏洞管理，合规，运行时防御，持续集成和持续交付，云原生防火墙和访问控制 |
| | 2019.5.30 | PureSec | Cloud Security | 替Serverless应用程式提供端对端的安全 |

*来源：公司官网，中国银河证券研究院整理*

图24 Palo Alto 详细战略布局

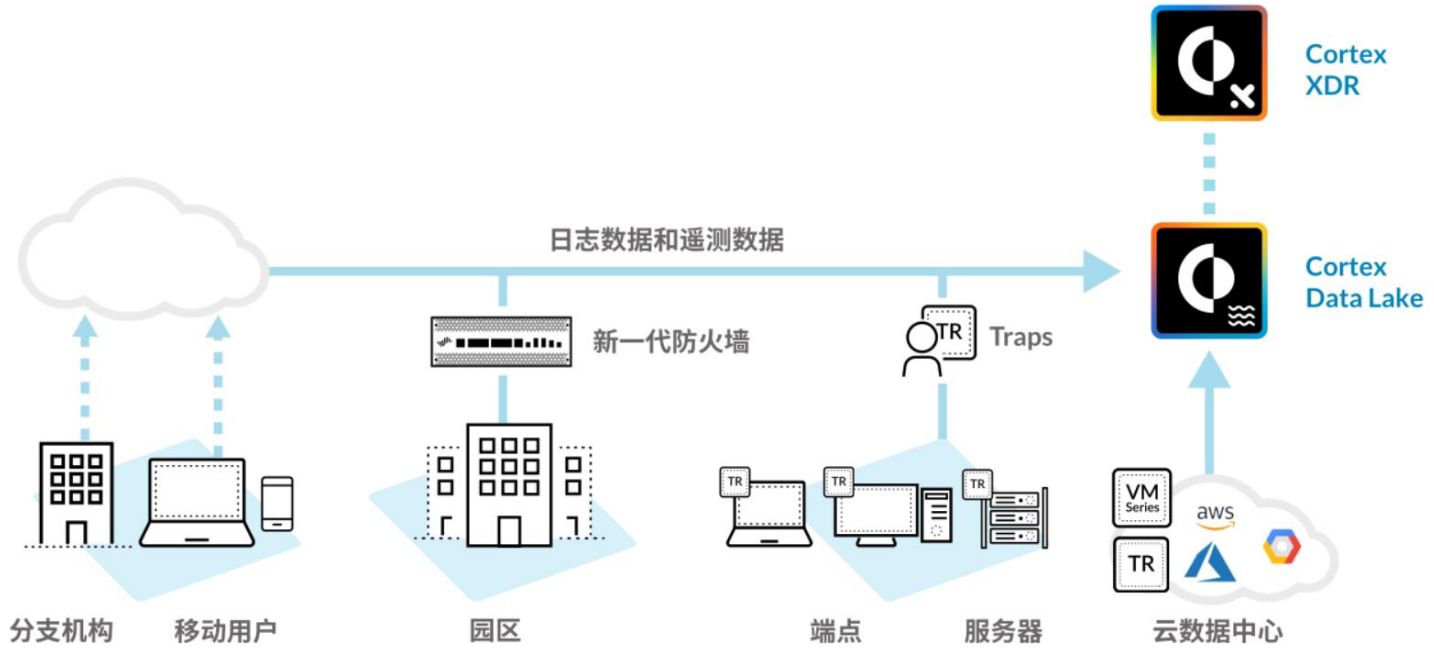
| 公司名称 | 详细战略 |
|---|---|
| Palo Alto Networks | 加强云安全领域，努力保持领导者地位，加强云合规性和云安全分析能力，实现完整持续的合规验证，发现资产，监测漏洞和风险，并实现事件调查与威胁修复 |
| | 继续现有对Cortex XDR、Prisma和Traps的研究，旨在更好的利用先进的人工智能和机器学习的力量 |
| | 建立Palo Alto Networks的应用框架，第三方的软件开发商可以通过开放API在此应用框架上进行开发，用户使用这些新产品、新功能的方式与使用苹果商店中的应用程序类似。 |
| | 推出全新的K2系列来应对5G市场，防止针对4G和5G移动网络、物联网设备和移动用户的高级网络攻击。 |
| | 新的合作伙伴计划NextWave Partner Program，简化计划级别、分层折扣结构和新的合作伙伴激励措施来发展其业务，旨在提高利润率和盈利能力。 |
| | 推进Palo Alto Networks网络安全学院，弥补网络安全人员短缺问题，寻求各政府部门及关键设施的合作协议，帮助他们构建安全的网络方案，应对越来越多的网络安全威胁 |

*来源：公司官网，中国银河证券研究院整理*

其**Cortex**是业界首个开放集成的人工智能持续安全平台，部署于全球性可扩展公有云平台之上，助力安全运维团队提高海量数据分析速度、简化安全运维工作。Cortex由**Cortex Data Lake** 驱动，该数据湖可安全存储客户私有数据并实现对海量数据的分析，借助高级人工智能和机器学习技术发现威胁并快速编排响应策略。

**Cortex XDR**通过Data Lake的网络、端点和云的关联数据简化检测和响应，节省了数小时的手动分析时间，并通过AI行为分析发现隐蔽性攻击，在发生破坏前对威胁进行分类和控制。可检测凭证窃取和 DNS 隧道威胁等传统方式无法识别的威胁。

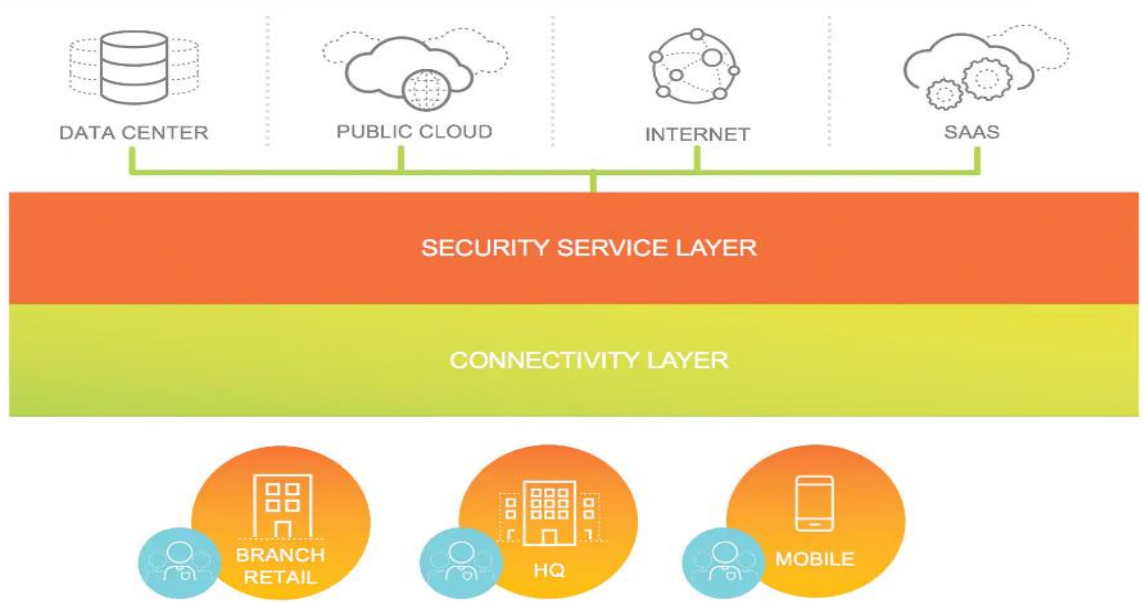
图25 Cortex XDR




*来源：公司官网，中国银河证券研究院整理*

**Prisma**有四款不同的产品：**Prisma Access**具有专为服务提供商而设计的简化的云管理用户界面，能为世界各地的分支机构和移动用户通过可扩展云原生架构提供安全的云访问。**Prisma Public Cloud**可以在整个云环境中将数据和风险进行相关评估，在公共多云部署上提供跨持续可见性、安全性和合规性监控。**Prisma SaaS**是一种多模式云访问安全代理服务，提供风险发现、自适应访问控制、数据丢失防护、合规性保证、数据治理、用户行为监控和高级威胁防护等功能。**Prisma VM**系列是Palo Alto Networks防火墙的虚拟化，可部署在私有云和公共云计算环境里。

图26 Prisma




*来源：公司官网，中国银河证券研究院整理*

# 1.4.3 Symantec布局

Symantec计划继续扩大端点防护和CASB方向的技术优势，将EDR和人工智能相结合，发展**MEDR**技术，自动化管理端点安全，减少响应与处理时间，同时延展端点防护外延，针对移动端以及物联网的信息安全提供解决方案。云安全方面跟进CASB的投入，包括收购微隔离公司**Fireglass**等。

图27 2017年起Symantec收购案例

| 公司名称 | 日期 | 收购对象 | 技术方向 | 详细说明 |
|---|---|---|---|---|
| Symantec | 2017.7.7 | Fireglass | Browser Isolation | 浏览器威胁隔离技术见长，通过防止恶意内容穿过防火墙 |
| | 2017.7.12 | Skycure | EDR | 扫描用户设备，寻找App、操作系统、以及网络等方面可能存在的安全漏洞 |
| | 2017.11.07 | SurfEasy | VPN | 增强对无线服务和免费Wi-Fi的安全保护 |
| | 2018.11.7 | Appthority | Security Mobile | 限制不需要的应用行为、法规合规性和评估漏洞 |
| | 2018.11.7 | Javelin Networks | Threat Protection | 保护微软Active Directory系统的部署，保存敏感的用户信息如帐户密码等 |
| | 2019.2.12 | Luminate | Cloud Security | 提供统一的安全堆栈，只允许点对点，临时用户访问跨环境和基础架构的特定公司资源 |

*来源：公司官网，中国银河证券研究院整理*

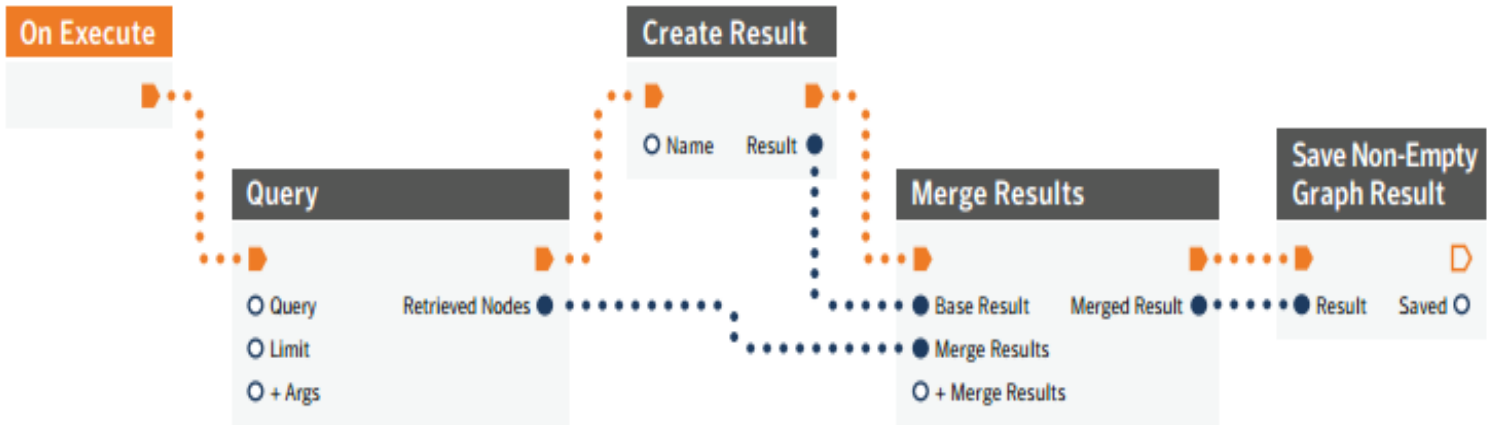
图28 Symantec详细战略布局

| 公司名称 | 详细战略 |
|---|---|
| Symantec | 继续建立庞大的客户基础来提供执行交叉销售策略和长期策略，继续向市场推广网络防御技术。 |
| | 推行新的托管端点检测和响应（MEDR）服务以及增强的EDR 4.0技术，使用AI驱动的分析和自动化来改进攻击发现和事件响应，以快速发现和阻止复杂的网络攻击 |
| | 重点关注云计算技术开发。尤其是CASB（云访问安全代理）和网络隔离技术方面 |

*来源：公司官网，中国银河证券研究院整理*

**MEDR** 该解决方案通过先进的机器学习技术集成了欺诈技术、移动威胁防御、终端检测和响应 (EDR) 等技术，建立在领Symantec Endpoint Protection 平台上，进一步强化提升了安全防御功能。

图29 MEDR




*来源：公司官网，中国银河证券研究院整理*

# 1.4.4 Fortinet布局

Fortinet的战略一方面增加在非研发方向上的投入，比如扩大对合作伙伴的激励以及建立网络学院培养人才储备；另一方面扩张对IoT以及OT方向上的投资，包括收购**ZoneFox**等公司，吸收UEBA和EDR技术扩张优势，以及推出IoT、车联网产品安全的解决方案等。

图30 2017年起Fortinet收购案例

| 公司名称 | 日期 | 收购对象 | 技术方向 | 详细说明 |
|---|---|---|---|---|
| Fortinet | 2018.6.4 | Bradford Network | EDR IoT Security | 基于策略的安全自动化和编排解决方案，将微隔离与安全管控扩展到了本地，提供无需代理的对所有接入网络设备的安全评估以及实时查看不受信设备的功能 |
| | 2018.10.23 | ZoneFox | UEBA | 扩展了用户实体行为分析（UEBA）功能，支持边界和云端部署。利用机器学习来检测异常行为，并对内部威胁提供更快的响应。 |

*来源：公司官网，中国银河证券研究院整理*

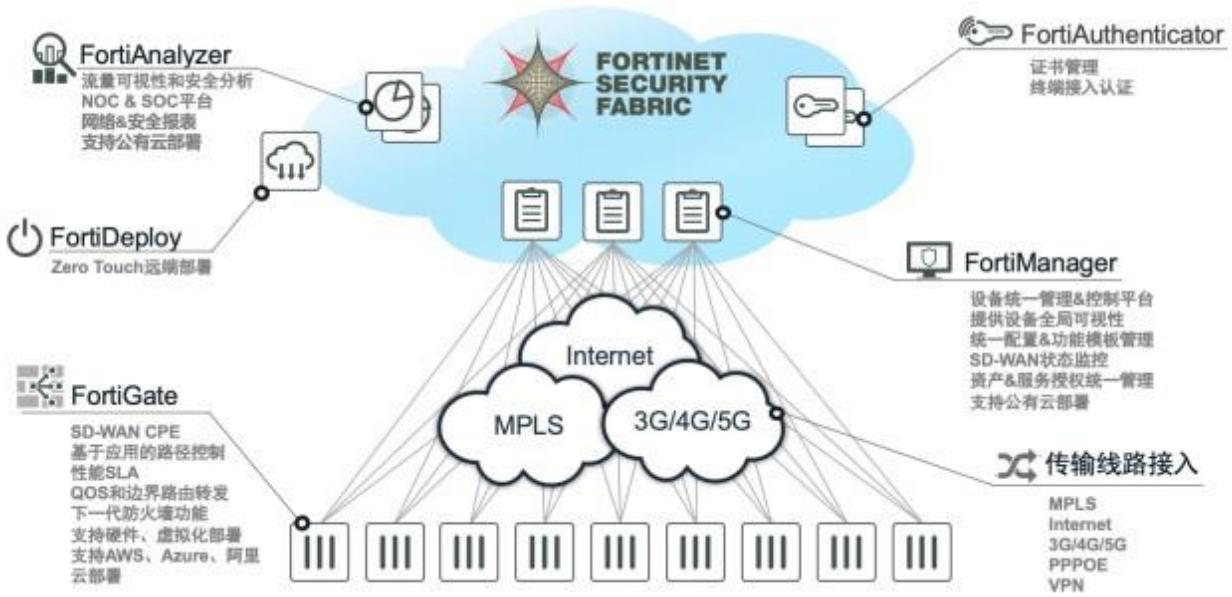
图31 Fortinet详细战略布局

| 公司名称 | 详细战略 |
|---|---|
| Fortinet | 投入生产新型SD-WAN ASIC芯片来加速部分产品的运行速度，包括FortiGate 100F Appliance等 |
| | 推广5G的安全保护以及在OT和IoT上的投资，研究联网汽车的集成安全和威胁保护解决方案 |
| | 寻求各政府部门及关键设施的合作协议，帮助他们构建安全的网络方案，应对越来越多的网络威胁 |
| | 建立更多的Fortinet网络安全学院（FNSA），与学术机构、非营利组织和资深项目合作，为参与者提供网络安全职业生涯所需的技能，弥补网络安全人员短缺问题。 |
| | 增加对合作伙伴和渠道计划的投资，试图获得市场份额（与合作伙伴关共赢），提高账户覆盖率。 |
| | 继续研究架构安全和群体智能。整合，协同，联动Fortinet各产品，在用户端构建一套足以和敌方抗衡的Fabric网络。 |

*来源：公司官网，中国银河证券研究院整理*

除去Fabric集成平台，Fortinet在基础网络端投入较大，如：着力于将防火墙与广域网连接起来的**SD-WAN+NGFW**，通过集成化 SD-WAN，帮助用户完善SD-WAN下的安全性、扩展性、性能、成本等方面的能力，帮助用户实现网络能力的一站式交付，统一运维管理，促进网络运维的持续简化。

图32 SD-WAN+NGFW




*来源：公司官网，中国银河证券研究院整理*

# 1.4.5 Check Point布局

Check Point Software战略以**Maestro**架构为核心，以应对5G带来的流量骤增，辅以对云安全、物联网安全方面的投入，收购**Dome9**完善特权身份保护等云安全功能，面对第六代网络安全的威胁，未来将会存在各个设备兼容的Nano Agents。

图33 Check Point Software 2017-2019年间主要收购对象

| 公司名称 | 日期 | 收购对象 | 技术方向 | 详细说明 |
|---|---|---|---|---|
| Check Point Software | 2018.10.24 | Dome9 | Cloud Security | 直观的安全态势可视化、合规性和管理自动化、特权身份保护PIM、云流量和事件分析，使云部署更安全、更易于管理 |
| | 2019.1.14 | ForceNock Security | WAAP | 以机器学习、行为和以声誉为基础的安全引擎 |

*来源：公司官网，中国银河证券研究院整理*

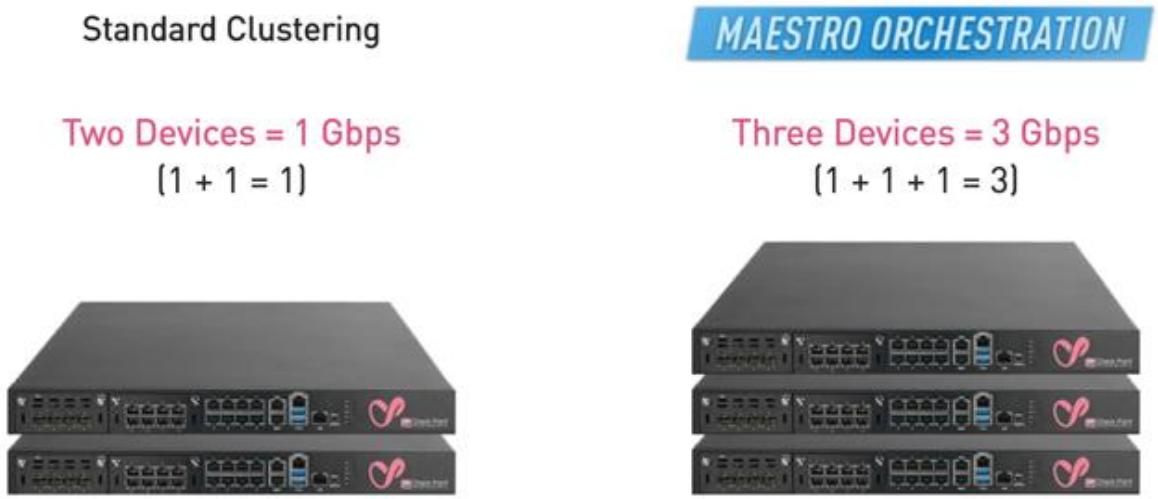
图34 Check Point Software 未来战略构想

| 公司名称 | 详细战略 |
|---|---|
| Check Point Software | 推行新的Maestro架构，使任何规模的企业都能享受灵活的云级安全平台的强大功能，并无缝地将现有的安全网关扩展到超大容量。 |
| | 构想针对“GEN VI”的网络安全服务，在每个设备、网络或云服务、应用程序和网络中部署Nano Agents代理防护，以保护未来的超连接、超尺度世界。 |
| | 推行新的全球合作伙伴计划Check PointS，直接奖励合作伙伴开展销售活动、加快销售周期并提供专家支持和资源。 |
| | 从对传统网络安全威胁信息的快速响应到提前预防潜在危险的革新，更好的应对云端威胁与云安全策略 |

*来源：公司官网，中国银河证券研究院整理*

Check Point推出**Maestro 架构**，将其现有的安全网关无缝扩展至超大容量，保护组织最大、资源需求最高的环境，包括超大规模数据中心、电信运营商和移动网络，同时可以使单个网关在几分钟之内扩张至50 倍宽度，能够为任何规模的企业提供服务。Maestro架构具有高度云计算化能力，可以在混合架构下更加智能、统一的布署安全性原则，提高工作性能同时降低人为错误。

图35 Maestro




*来源：公司官网，中国银河证券研究院整理*

# 1.5 Gartner安全十大项目布局



随着技术不断地发展，触发了大量新的安全需求，安全的边界在不断地拓宽。综合Gartner近几年预测来看，最新前瞻的技术集中领域主要有**云安全**、**端点安全**、**物联网**以及**安全运营**。

- 特权身份保护：PAM旨在让攻击者更难访问**特权账户**，并让安全团队监测到异常访问的行为，通过要求对所有管理员和承包商等外部第三方的访问实施强制多因素认证为组织的关键资产提供安全的特权访问。
- CASB：CASB主要针对公有云带来的**数据管控问题**，以及其衍生出的影子IT（Shadow IT）和BYOD（Bring your own device）问题。
- 容器安全：容器安全包括开发阶段的风险评估和对容器中所有内容信任度的**评估**，也包括投产阶段的运行时威胁防护和访问控制。
- CSPM：CSPM能够对IaaS，以及PaaS，甚至SaaS的控制平面中的基础设施安全配置进行分析与**管理**，包括账号特权、网络和存储配置、以及安全配置。
- EDR：EDR工具通常记录大量端点级系统的行为与相关事件，并将这些信息存储在终端本地或者集中数据库中。然后对这些数据进行IOC比对，行为分析和机器学习，用以持续对这些数据进行分析，快速对攻击进行**响应**
- BEC：BEC指代高级的、复杂的、高度定向的**邮件钓鱼攻击**，通常针对公司财务相关人员，通过社会工程学和网络入侵等各种方式，诱骗相关人员将钱转入犯罪分子银行账户。
- SOAR+SIEM：安全编排、自动化及响应(SOAR)，旨在**快速检测响应**威胁、减少安全人工分析投入、提高安全运营的效率。安全信息和事件管理（SIEM）通过对来自**安全事件**的实时收集和历史分析来支持威胁检测和安全事件响应。
- 弱点评估与管理修复：采用仿真黑客行为模式的**人工智能扫描技术**,针对暴露在网络上的主机与网络服务信息进行扫描分析,有效祢补一般网络安全扫描工具的缺点与被忽略的问题。

对比过去五年10大安全项目，19年全新上榜的包括安全事件响应和安全评级服务以及隔年再次上榜的容器安全。同比国外安全行业，国内企业产品布局有所差距。

图36 Gartner十大项目

| | |
|---|---|
| 特权账户管理 | Palo Alto、Check Point、Fortinet、深信服、启明星辰、奇安信 |
| 云访问安全代理（CASB） | Palo Alto、Check Point、Fortinet、深信服、启明星辰、奇安信 |
| 容器安全 | Palo Alto、Fortinet |
| 云基础安全配置与管理（CSPM） | Palo Alto、Check Point、Fortinet、启明星辰 |
| EPP+EDR | Palo Alto、Check Point、Fortinet、深信服、启明星辰、奇安信 |
| 商业邮件失陷（高级主动邮件反钓鱼） | Palo Alto、Check Point、Fortinet、启明星辰 |
| SIEM+SOAR | Palo Alto、Check Point、Fortinet、启明星辰 |
| 弱点评估与管理修复 | 启明星辰 |

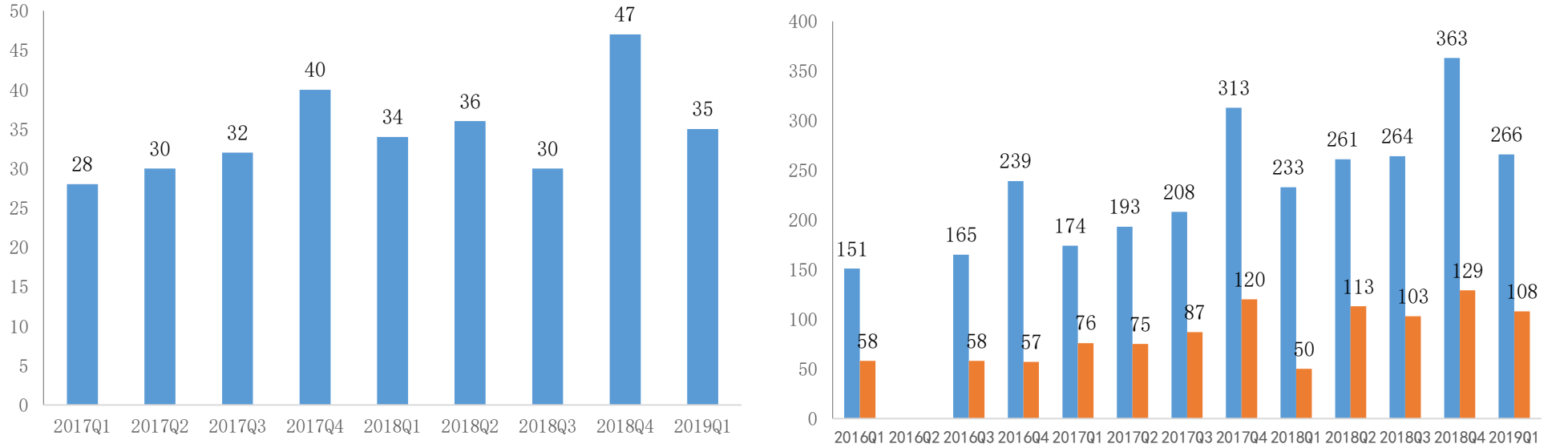
*来源：公司官网，中国银河证券研究院整理*

# 2. 安全巨头订单趋势不断增大



在纷纷推出网络安全产品集成平台之后，以Fortinet为例，自然季度2017Q1至2019Q1期间，Fortinet超过一百万美元的订单数量与时间呈现一定的正相关性，头部订单数量持续增长，取Fortinet2016Q1到2019Q1十二个季度的订单大小数据，大于25万美元订单和大于50万美元订单的同比增长率估计值超过了Fortinet自身季度营收增长率5.13%，在大于25万、50万和100万美元目标上，我们认为原因是随着下一代NGFW及其一体化架构的投入市场，消费者的投资偏好由多公司分产品单独购买变为采用单一公司的一体化平台。此外，Fortinet营业收入按产品线拆分，下一代防火墙硬件FortiGate为收入核心，其次为一体化架构Infrastructure Fabric，具体包括Fabric中的各项额外增值安全应用以及相关服务。在Infrastructure的用户群体中，亚太地区及拉丁美洲贡献了主要的增长驱动力。

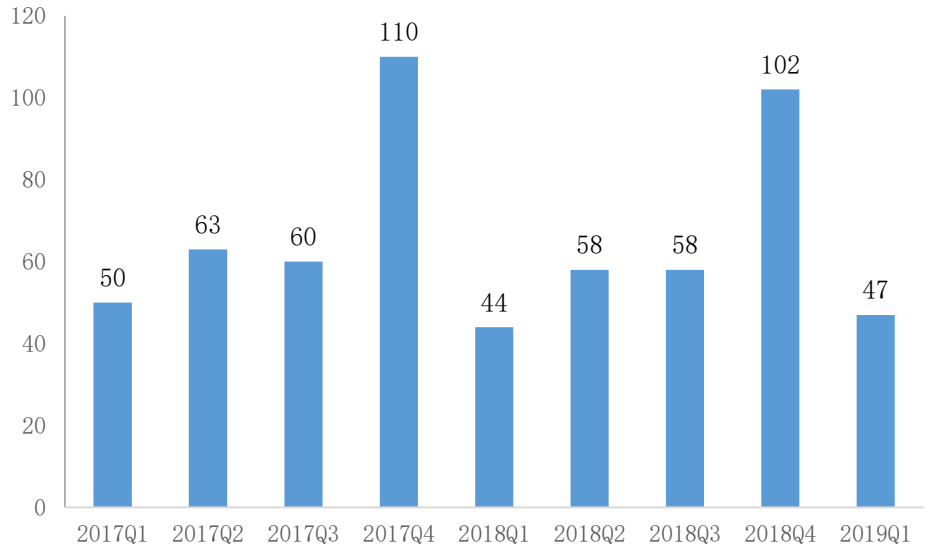
图37 Fortinet大于一百万美元订单数量




*来源：Wind，Bloomberg，中国银河证券研究院整理*

Check Point的大额订单数量同季度对比有略微下降，考虑到自身市占率下滑，超过100万美元的订单数量下降程度在可接受范围内，并且2018年公司多次披露大额订单的总价值呈不断上涨趋势，结合数量证明存在头部订单数额攀升情况，客户更加趋向与购买全面的Infinity一体化架构。2018年度，Infinity产品递延收入由13.3亿美元增长至14.89亿美元，同比增长1.61亿美元，增速达到11.9%，预期将会构成Check Point营业收入的主要成长点。

图38 2017Q1-2019Q1check Point大额订单情况



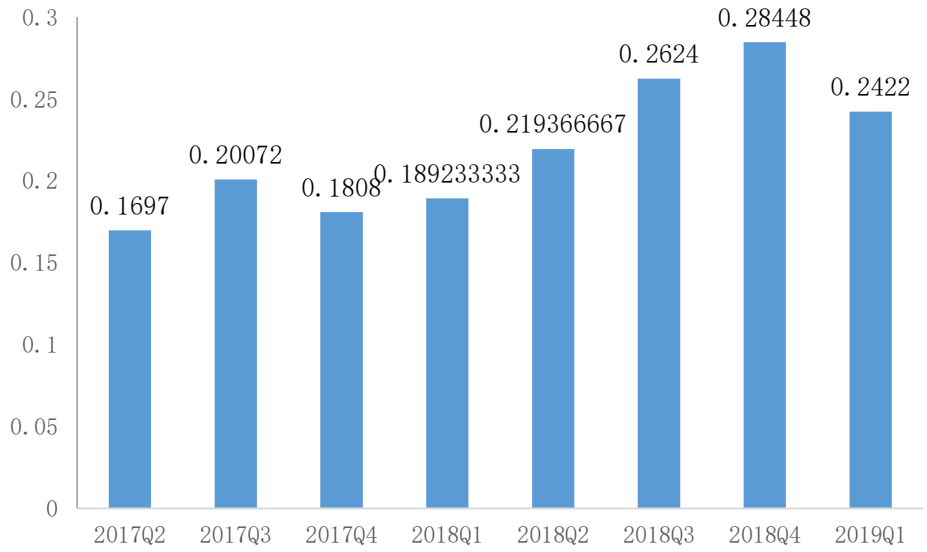

*来源：公司官网，公司报告，中国银河证券研究院整理*

# 2. 网络安全企业订单收入变化



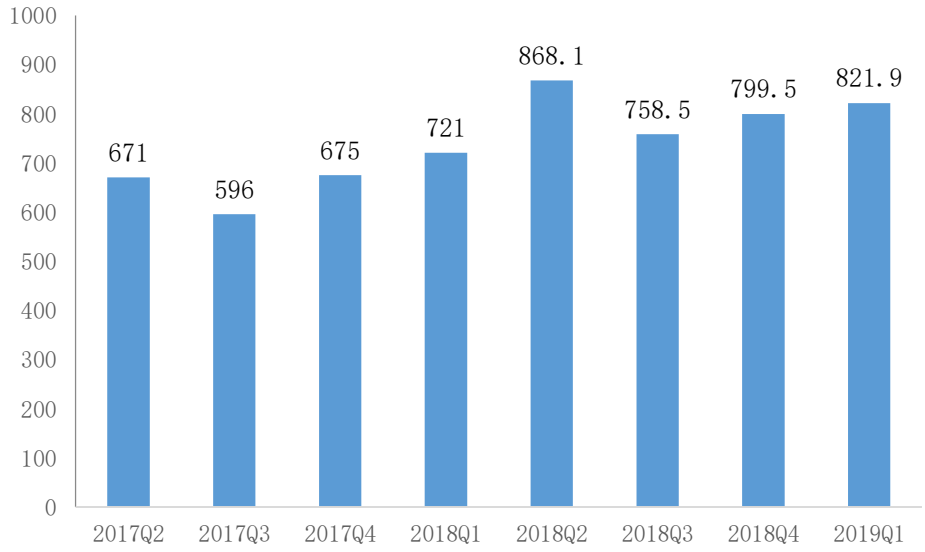
自然季度2017Q2-2019Q1，Palo Alto每新增用户平均收入（总营收/新增用户数量）由17万美元增长至24万美元，在2018Q4达到了28万美元的峰值，结合订单由6.71亿美元增长至8.22亿美元的走向，我们认为用户群体在选择网络安全厂商时单次订单的签订金额呈上升趋势，在选择Palo Alto下一代防火墙的同时，订阅了更多的SaaS产品。

图39 Palo Alto每新增用户平均收入




来源：公司官网，公司报告，中国银河证券研究院整理

图40 Palo Alto签订订单总计金额情况



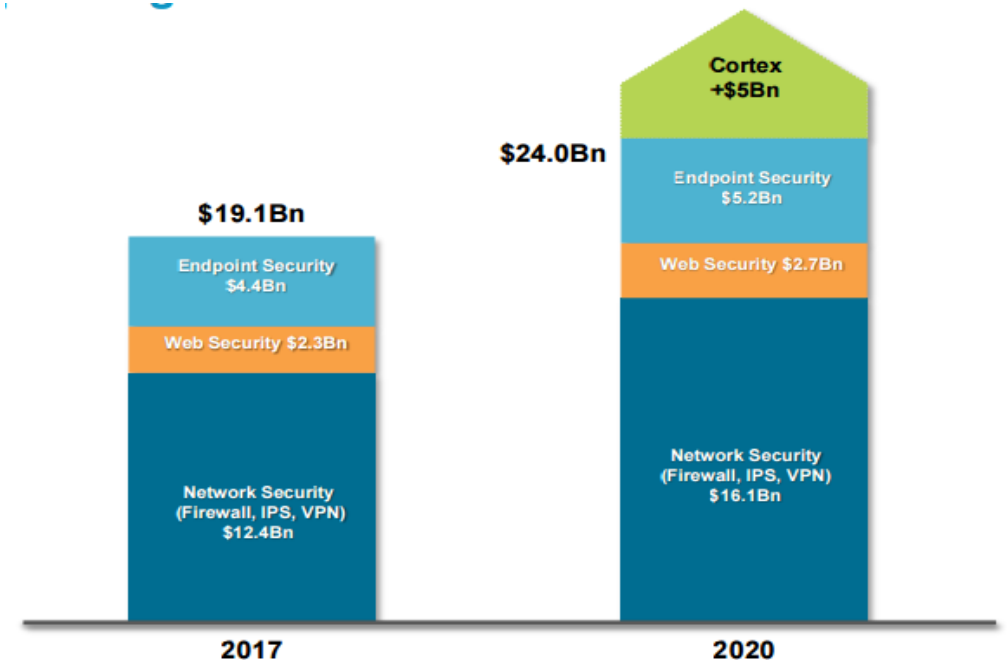

来源：公司官网，公司报告，中国银河证券研究院整理

# 2. 网络安全企业订单收入变化



2019Q1季度，Palo Alto与现有的网络安全厂商客户达成了十起超过五百万美元的订单，并与美国政府机构签订了历史级的八位数的大额订单，订单内容包括硬件替换以及新一体化安全平台的应用，新产品Cortex XDR达成包括一起百万美元级在内的总计五十份订单，Palo Alto预计Cortex将为网络安全市场带来额外的50亿美元空间。

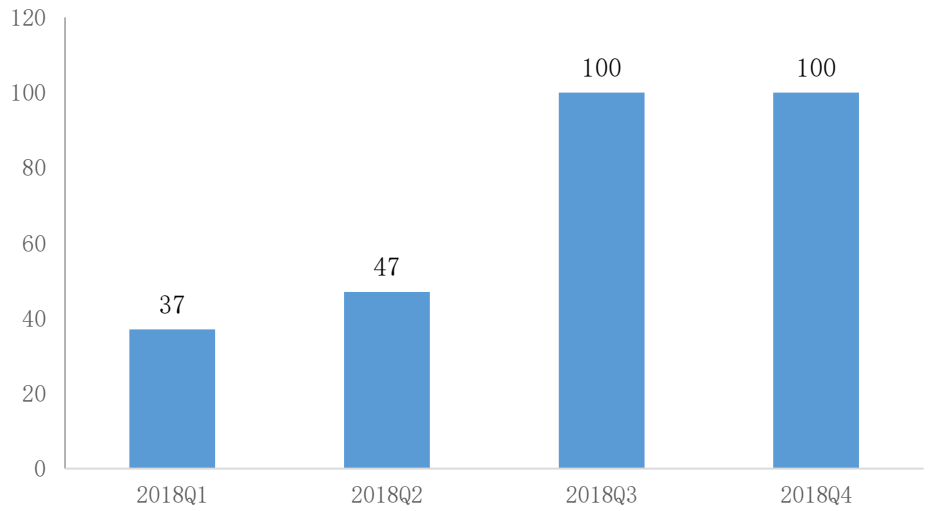
图41 SD-WAN+NGFW




*来源：IDC，Palo Alto，中国银河证券研究院整理*

2018财年，赛门铁克超过百万美元订单数量上升巨大，由2018Q1的37起上升至2018Q4的100+起，同时2019财年赛门铁克与一家欧洲家用硬件厂商达成了一起关于最新的一体化解决方案Integrated Cyber Defense Solution的千万美元级订单。一体化架构使得客户订单集中化，大额化，帮助赛门铁克达成更多的订单收入。

图42 赛门铁克2018财年订单数量




*来源：公司官网，中国银河证券研究院整理*

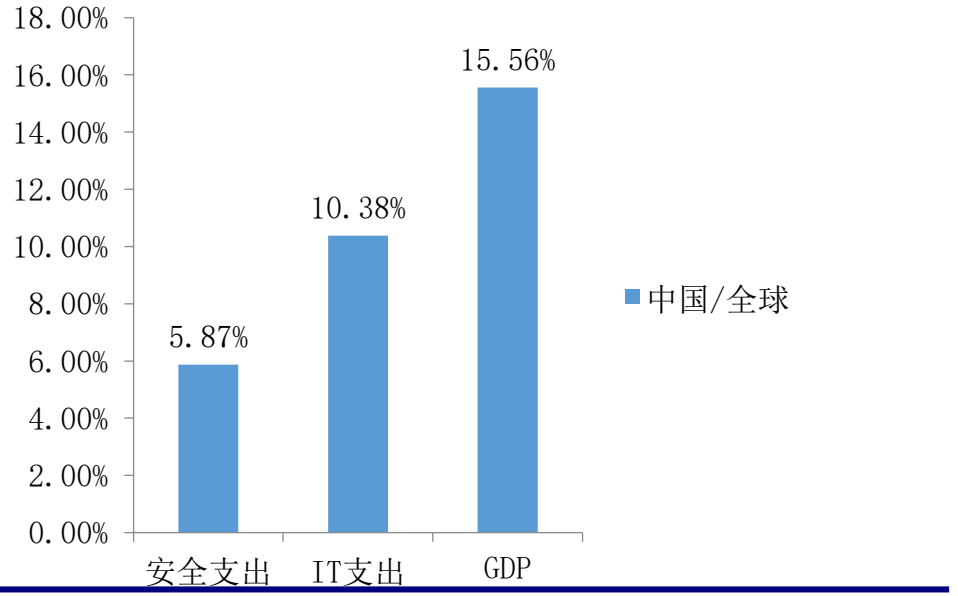
相比非一体化的安全产品，一体化架构在安全防护上、产品兼容性上都远远胜出，更适合部门层级复杂的机构用户，因此在购买抉择上会呈现偏好一体化架构的倾向，预计在近五年内，网络安全市场更多的表现出集中化特质，大额订单数量和质量增长，龙头企业赢得更多市场份额。

# 3. 对比海外，国内网安行业有较大提升空间



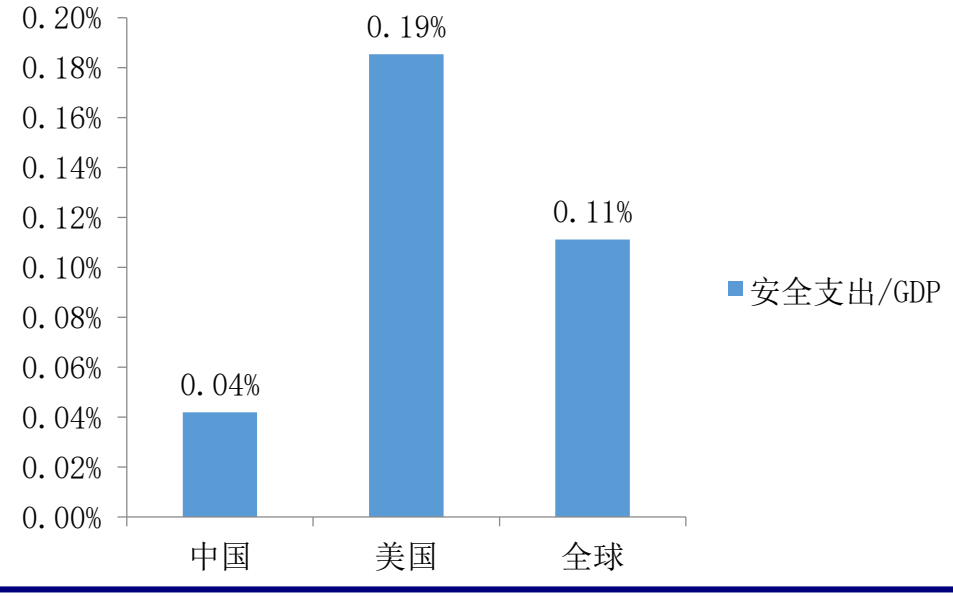
我国作为全球第二大经济体，网络安全方面的支出水平远低于世界平均水平。2018年，我国GDP占全球的15.56%，IT支出占全球的10.38%，而安全支出仅占全球的5.87%；我国安全支出占GDP的0.04%，而美国安全支出占GDP的0.19%，世界平均水平为0.11%。因此，考虑我国当前的经济体量，网络安全市场还有极大的发展空间。

图43 2018年中国市场与全球市场对比




*来源：Wind，中国银河证券研究院整理*

图44 2018年中国市场与美国市场、全球市场对比




*来源：Wind，中国银河证券研究院整理*

# 3.1 等保2.0提振行业增速

除了安全支出比例低于全球平均水平，我国的网络安全法规也还处于不断完善的过程中，网络安全法规的发展催生了新的安全需求，推动国内安全行业市场的扩张。

图45 等级保护发展历程

| 时间 | 具体内容 |
| --- | --- |
| 1994年 | 《中华人民共和国计算机信息系统安全保护条例》（国务院令147号） |
| 1999年 | 《计算机系统安全保护等级划分准则》 |
| 2004年 | 《关于印发<关于信息安全等级保护工作的实施意见>的通知》（公通字［2004］66号） |
| 2007年 | 《信息安全等级保护管理办法》（公通字［2007］43号）<br>《信息安全等级保护备案实施细则》（公信安［2007］1360号） |
| 2008年 | 《公安机关信息安全等级保护检查工作规范》（公信安［2008］736号） |
| 2010年 | 《关于动信息安全等级保护测评体系建设和开展等级测评工作的通知》<br>《关于开展信息安全等级保护专项监督检查工作的通知》（公信安［2010］1175号） |
| 2012年 | 《国务院关于大力推进信息化发展和切实保障信息安全的若干意见》（国发［2012］23号） |
| 2014年 | 《关于加强国家级重要信息系统安全保障工作有关事项的通知》（公信安［2014］2182号） |
| 2016年 | 《国民经济和社会发展第十三个五年规划纲要》“十三五”国家信息规划 |
| 2017年 | 《中华人民共和国网络安全法》 《全国电子政务外网工作2018年工作重点》 |
| 2019年 | 等级保护2.0落地 |

*来源：公安部，国务院，中国银河证券研究院整理*

网络安全等级保护是指对国家重要信息、法人和其他组织及公民的专有信息以及公开信息和存储、传输、处理这些信息的信息系统分等级实行安全保护，对信息系统中使用的信息安全产品实行按等级管理，对信息系统中发生的信息安全事件分等级响应、处置。

图46 等级保护划分

| | |
|---|---|
| 第一级 | 信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。 |
| 第二级 | 信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。 |
| 第三级 | 信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。 |
| 第四级 | 信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害。 |
| 第五级 | 信息系统受到破坏后，会对国家安全造成特别严重损害。 |

*来源：公安部，中国银河证券研究院整理*

图47 等保2.0变化

| 变化 | 具体内容 |
| --- | --- |
| 名称变化 | 名称上由“信息安全等级保护”转变为“网络安全等级保护”。 |
| 法律效力变化 | 等保1.0是以1994年国务院颁布的147号令《计算机信息系统安全保护条例》为立法依据的行政法规。等保2.0则是以经过全国人大通过的《中华人民共和国网络安全法》为立法依据。 |
| 保护对象变化 | 等保1.0主要包括基础网络和信息系统，而等保2.0将大数据中心、云计算平台、物联网、工控系统、公众服务平台、互联网企业等全部纳入等级保护监督。 |
| 工作内容变化 | 等保1.0工作内容主要由五个规定性动作组成，为定级、备案、建设整改、测评和监督检查。而等保2.0在此基础上增加了风险评估、安全监测、通报预警、事件调查、数据防护、灾难备份、应急处置、自主可控、供应链安全、效果评价、综治考核等项目。 |
| 控制措施分类变化 | 等保2.0由旧标准的10个分类调整为8个分类，分别为技术部分：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；管理部分：安全策略和管理制度、安全管理机构和人员、安全建设管理、安全运维管理。 |
| 定级备案流程变化 | 等保1.0定级原则是“自主定级、自主保护”。而等保2.0则采取了专家评审，主管部门审核的方式。将原有的30天内备案缩短为10个工作日，并明确了定级流程分为：确定定级对象、初步确定等级、专家评审、主管部门审核、公安机关备案。 |
| 测评周期与测评要求的变化 | 等保2.0则要求网络运营者选择符合国家规定条件的测评机构，对三级以上系统每年开展一次等级测评，对四级系统测评周期有所放宽。等保1.0要求60分基本合格，等保2.0要求75分以上为基本合格。 |
| 其他典型变化 | 等保2.0增加了可信计算的相关要求。 |

*来源：公安部，中国银河证券研究院整理*

根据IDC数据，预计到2022年，中国网络安全市场体量将达到近140亿美元，2018-2022年五年间复合增长率维持在25%，等保2.0提振约4个百分点；而全球网络安全市场2018-2022年五年间平均年增长率维持在9%左右，国内网络安全市场增速远高于全球平均水平，市场前景广阔。

图48 中国网络安全市场体量（百万）与增长率


来源：IDC，中国银河证券研究院整理

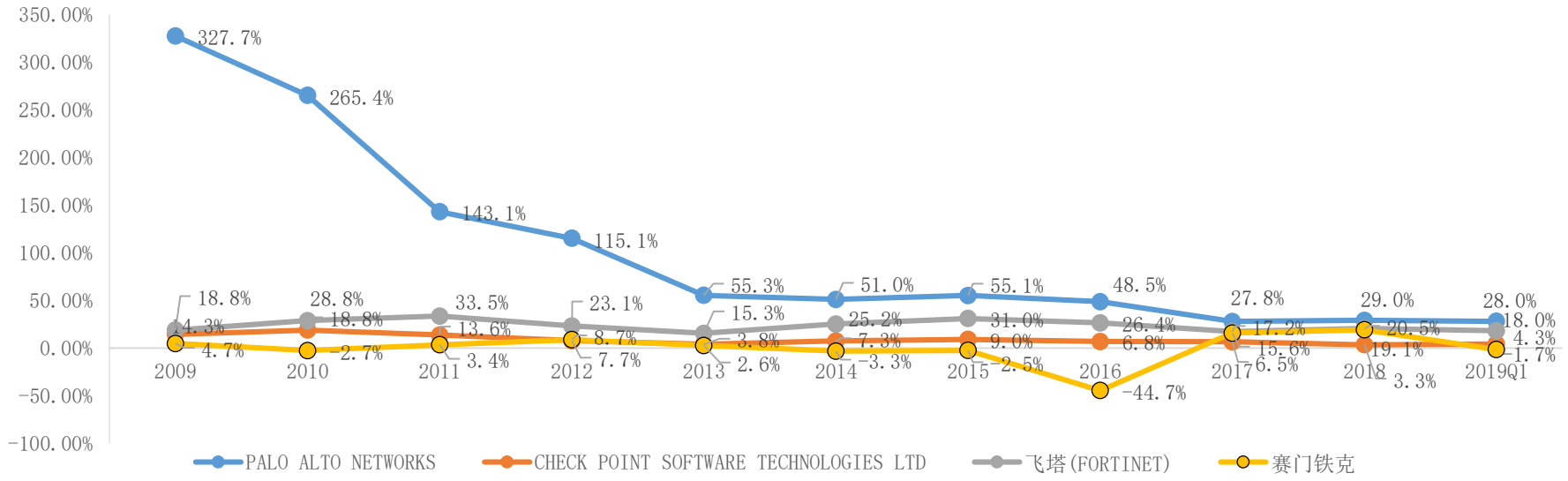
图49 全球网络安全市场体量（百万）与增长率


来源：IDC，中国银河证券研究院整理

# 3.2 对比巨头，我国网安公司收入差距大

- Palo Alto Networks在2013年之前处于**高速增长阶段**，主要得益于公司基数小，全新定义下一代防火墙，2013年之后收入仍保持高增长。
- Check Point和Fortinet收入增速**长期保持稳定**， Check Point由于2013年宏观环境较差，高端产品难以销售，虽然到了二、三季度，数据中心客户有所增长，但是2013年全年增长速度放缓。
- 赛门铁克由于2016年公司拆分**剥离数据存储业务部门**导致收入下滑，但近几年客户对端点防护的重视，有效推动收入较快增长。

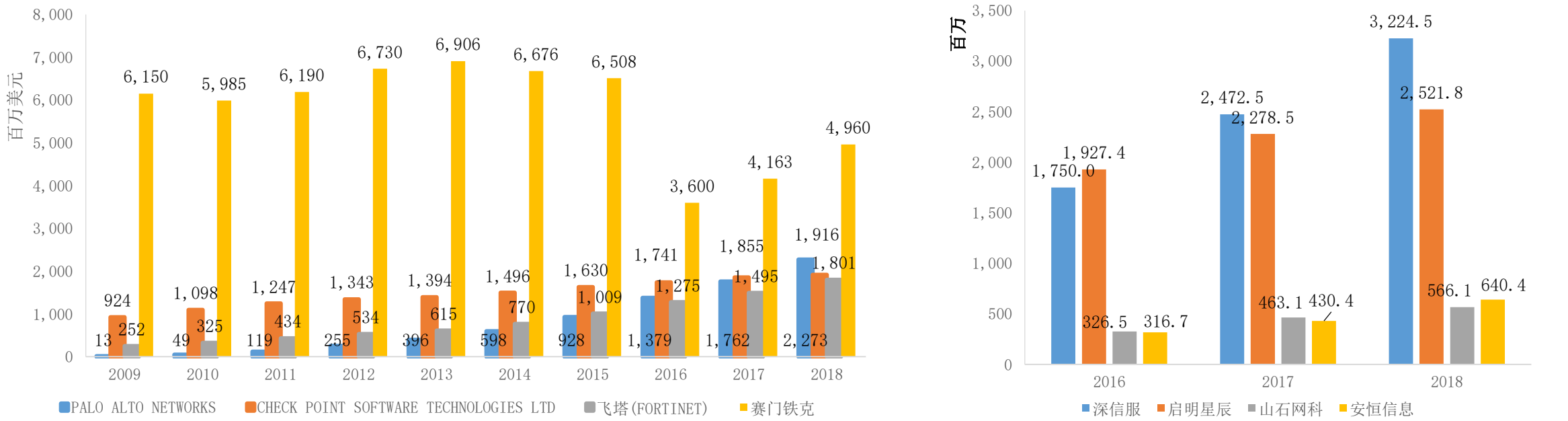
图50: 全球网络安全巨头2009-2018年收入增速变化




*来源：公司官网，中国银河证券研究院整理*

四家国内厂商较对标的海外网络安全领军企业差距明显，营业收入最高的深信服也只有海外营收最低的Fortinet的1/3。总的来说，和国外公司相比，我国网络安全企业的发展空间还很大。

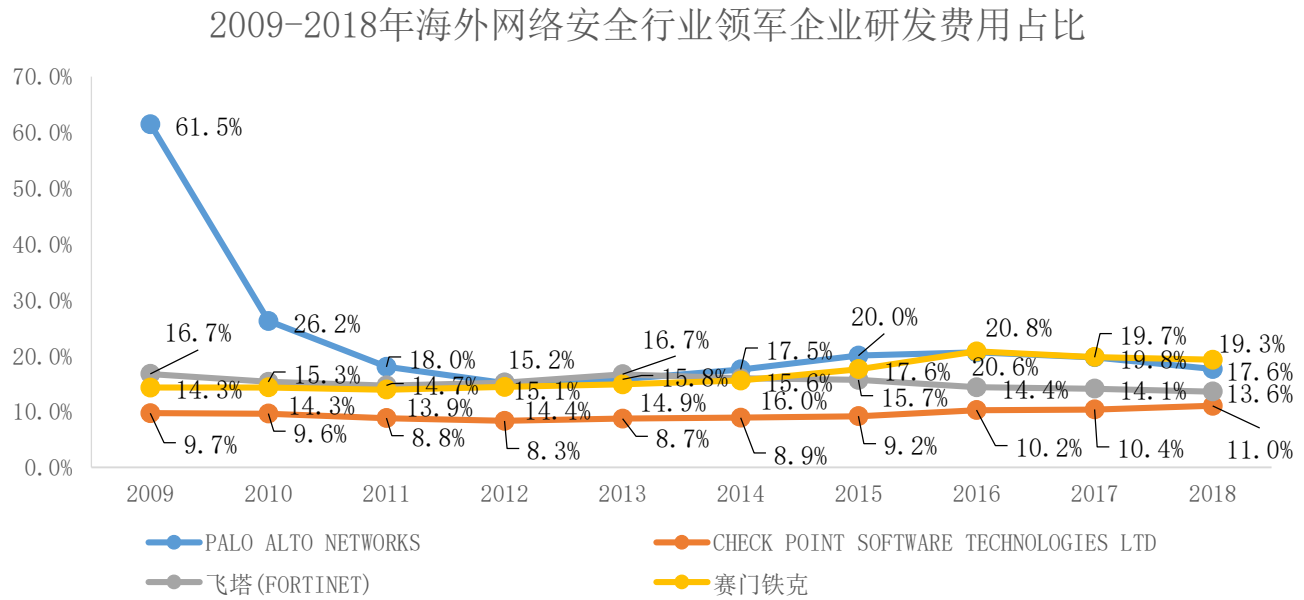
图51: 全球网络安全巨头2009-2018年收入水平




来源：公司官网，中国银河证券研究院整理

四家企业在研发中的投入稳中有升，Palo Alto在收入高增速的同时，基本维持20%的研发投入；赛门铁克在拆分之后，也基本维持20%的研发投入；Check Point近几年也大量投入在Gen-VI安全防护研发之中，利用设备中部署的Nano Agent可以在使用云网关的同时，有效防止敏感数据停留在企业之外。

图52: 全球网络安全巨头2009-2018年研发费用率

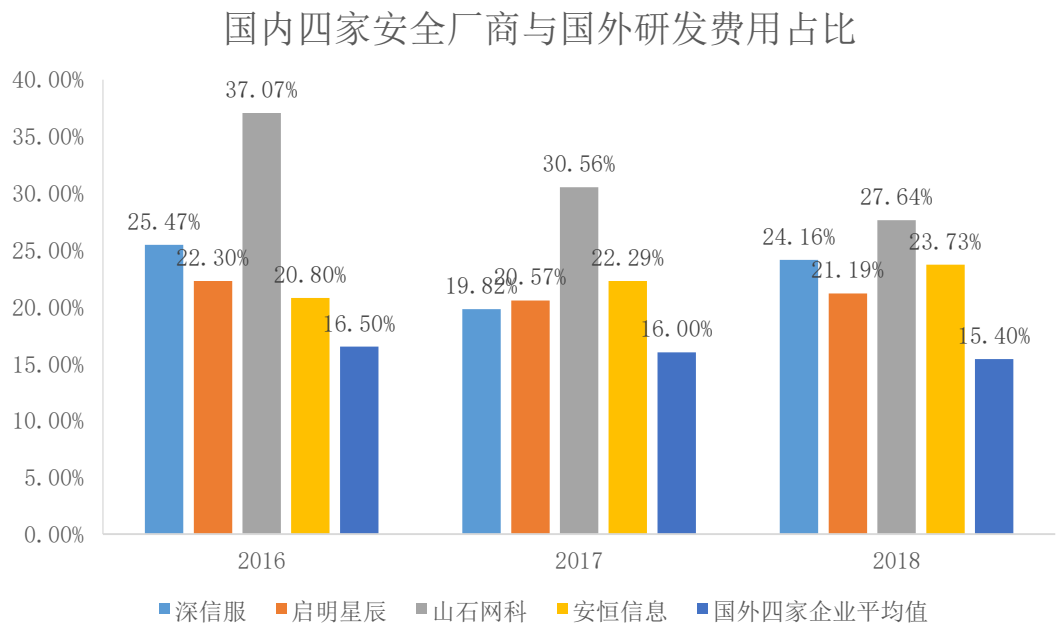


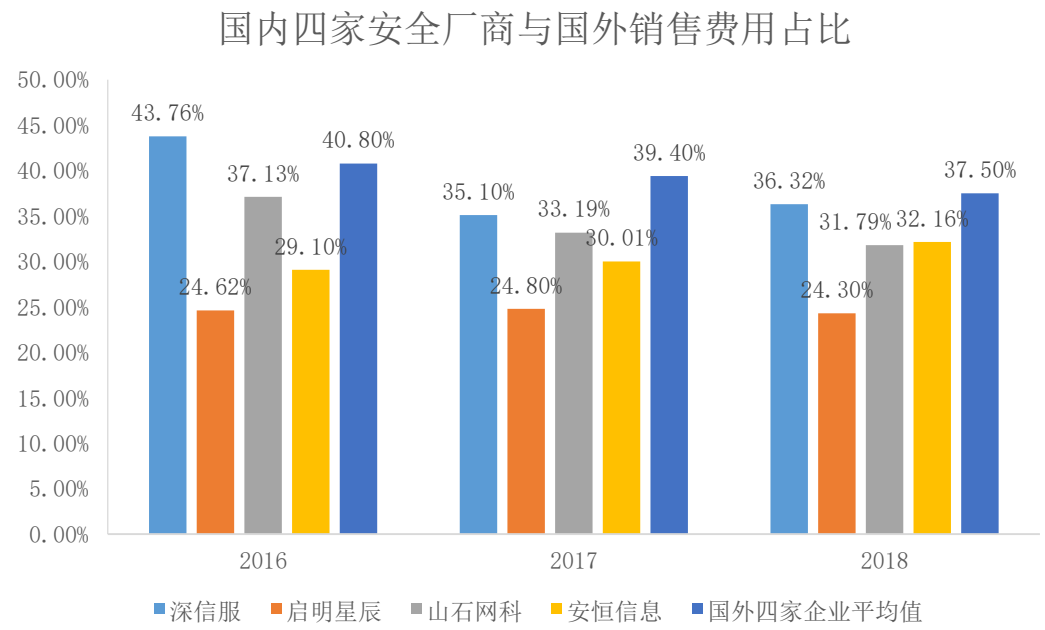

来源：公司官网，中国银河证券研究院整理

四家安全厂商销售费用占总体营收的比值逐渐下滑，研发投入维持在全行业较高的水准上（四家企业均连续三年超过20%收入比），相比国外四家安全行业领军者研发收入基本维持在10%-20%的区间，国内安全厂商还处于技术投入期，投资潜力较大，同时国内厂商中深信服与安恒信息营业收入迅速上扬的同时，研发占比并没有受影响而减少，两家公司有意识的维持跟进研发投入，保持技术优势。

和国外公司相比，国内安全厂商的销售费用率较低，大量资金投入于产品研发方面，可以期待未来的研发回报。

图53: 网络安全厂商研发销售费用率

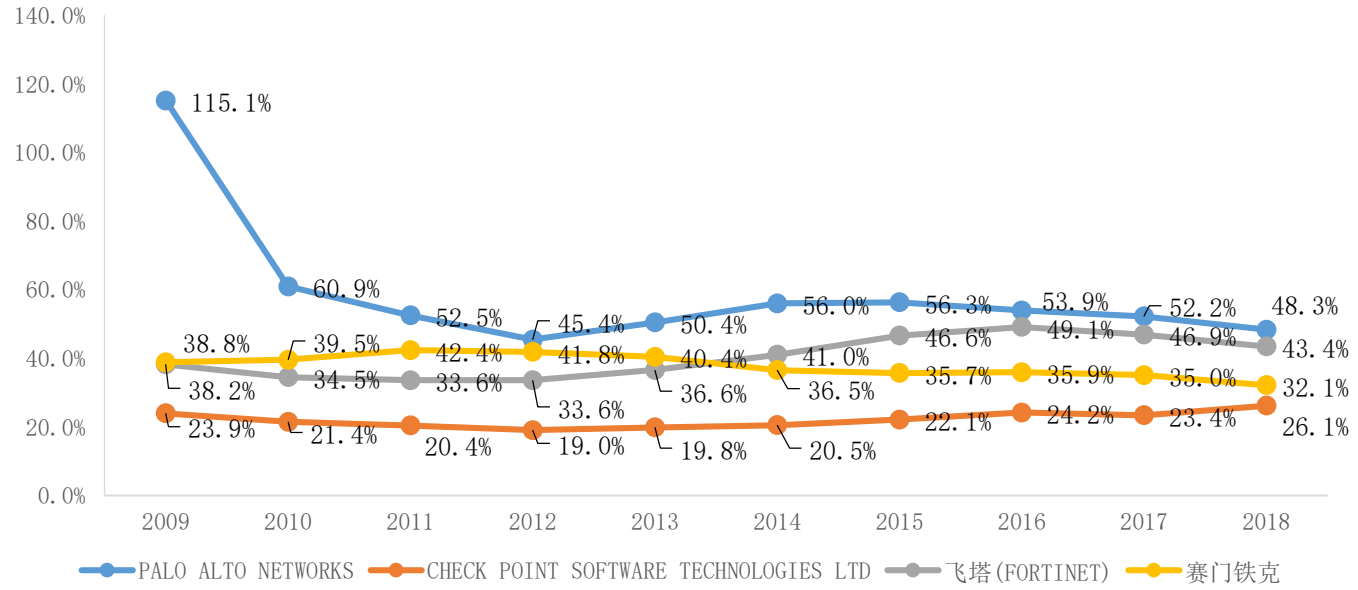



*来源：公司官网，中国银河证券研究院整理*

四家公司的销售费用占比都相对比较**稳定**，Fortinet和Symantec这两家公司的销售费用占比不相上下，10年来都在40%上下浮动。而Check Point则基本处于20%左右，尽管近年来略有上升的趋势，但总体依旧稳定。Palo Alto Networks公司相对成立时间较短，销售费用率**高于行业平均水平。**

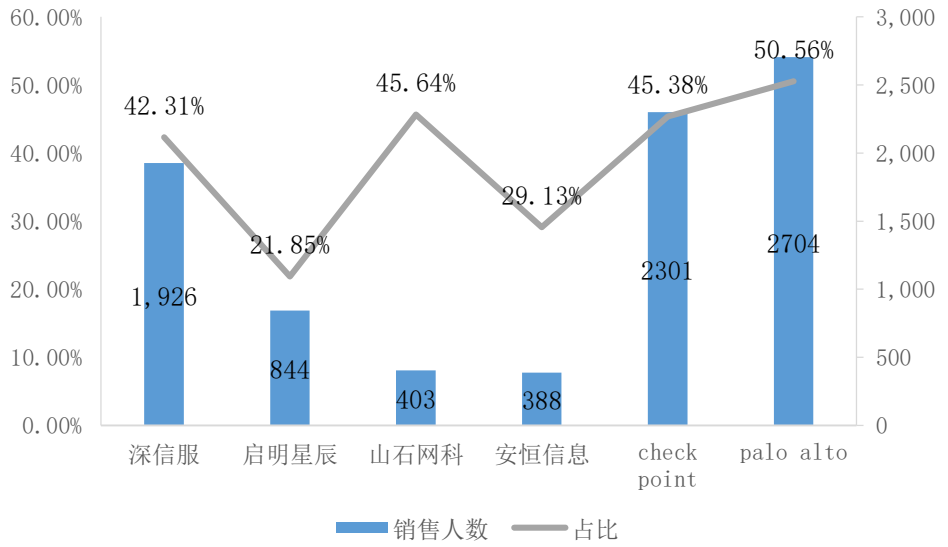
图54: 全球网络安全巨头2009-2018年销售费用率




*来源：公司官网，中国银河证券研究院整理*

国内安全厂商销售人员无论从人员总数还是占比，总体来说较低于国外领先安全厂家。

图55 销售模式




*来源：公司官网，中国银河证券研究院整理*

大部分的安全厂商采用分销为主的销售模式，少部分厂商的订单主要来自于直销，而Symantec还有自己的电商平台。

图56 销售模式

| | |
|---|---|
| Fortinet | 分销 |
| Check Point | 分销 |
| Palo Alto Networks | 分销为主，部分VM系列虚拟防火墙订单采用直销模式 |
| Symantec | 直销、分销相结合 |
| 深信服 | 分销为主 |
| 启明星辰 | 直销与分销相结合，直销业务占多半 |
| 山石网科 | 渠道代理销售为主、直销为辅 |
| 安恒信息 | 直销与分销相结合，分销业务占多半 |

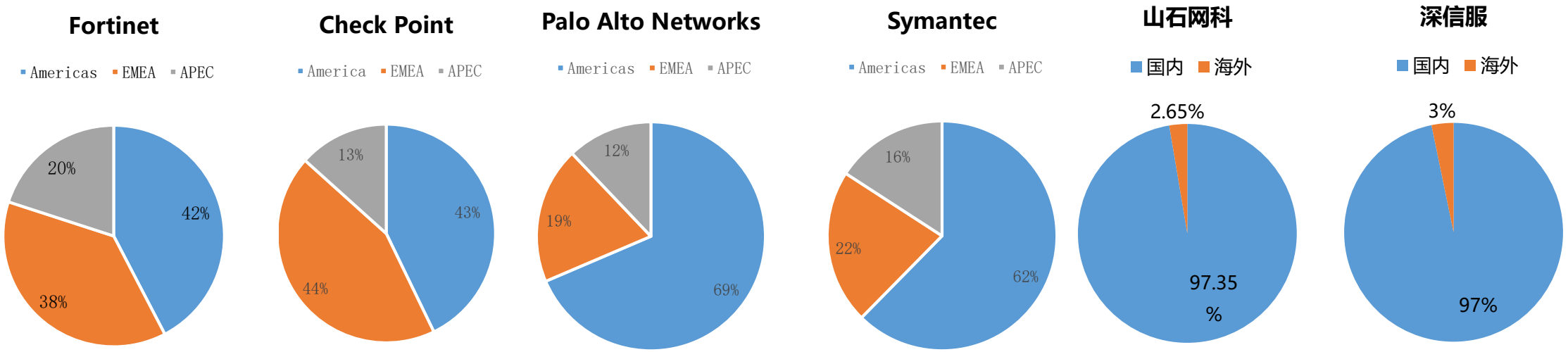
*来源：公司官网，中国银河证券研究院整理*

# 3.3 海外市场渗透率有待提升

国外安全厂商由于先发优势，采取全球发展策略，在亚洲、欧洲、北美市场均有规模以上收入。 国内安全厂商业务局限于国内市场，海外市场份额极少，还有极大的发展空间。

- 受公司战略影响， Fortinet和Check Point的营业收入核心来自于**美洲区和欧盟区**。Check Point主要采用合作的方法开拓市场，去年宣布与Blackberry合作，共同经营北美和欧洲的企业移动设备安全市场。Fortinet的总部在美国，依靠收购开拓市场，在去年10月份收购了欧洲的云端威胁分析公司ZoneFox。
- Palo Alto Networks和Symantec的营收大部分来自于**美洲区**。Palo Alto Networks的总部位于美国，多年来深耕美洲市场，近年来，公司大力发展全球网络范围计划，并于2018年在悉尼建成一个新设施。Symantec于2018年在北美发布新产品North Core，进一步巩固北美市场，同年七月，在印度金奈建成新的安全管理中心，以进一步开拓亚太市场。
- 深信服和山石网科率先布局海外市场，目前海外营业收入占到总营业收入的3%左右。

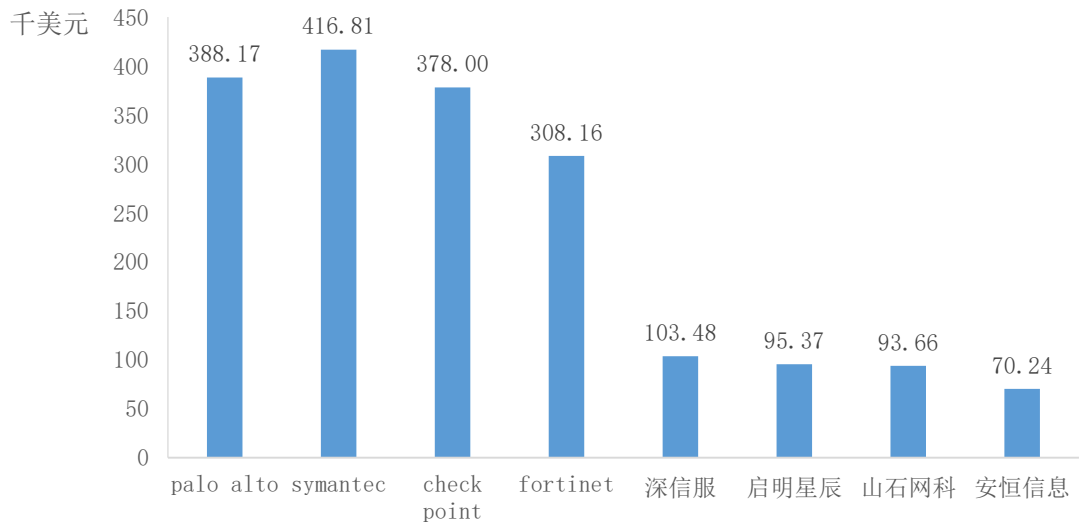
图57: 营收地域分布情况




来源：Bloomberg，中国银河证券研究院整理

根据2018自然年度网络安全厂商披露的营业收入和职工数量，深信服等四家厂商人均产出维持在十万美元波动，海外四家龙头企业的人均产出以高于三十万美元的数额超过国内安全厂商三倍有余。国内网络安全厂家人均产出仍有成长空间 。

图58 2018年度海内外八家网络安全厂商人均产出



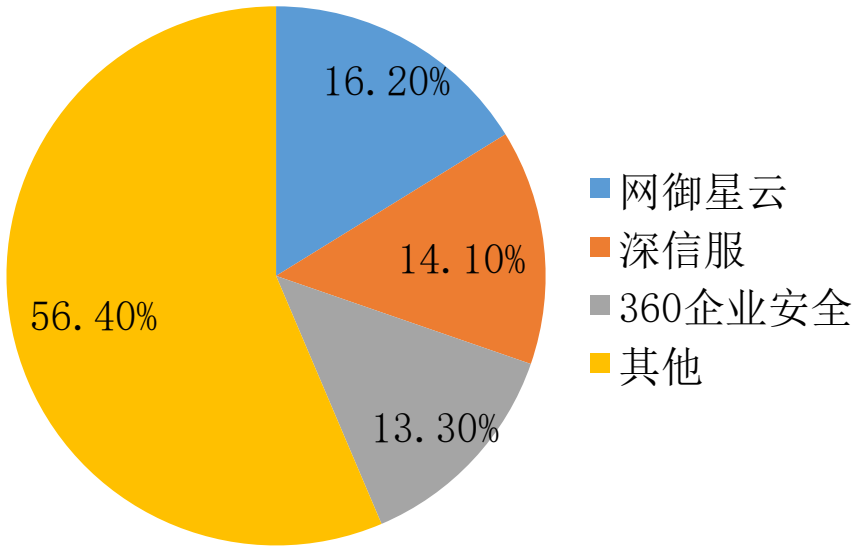

*来源：公司官网，中国银河证券研究院整理*

# 4. 标的推荐

## 4.1 国内网络安全市场份额概况

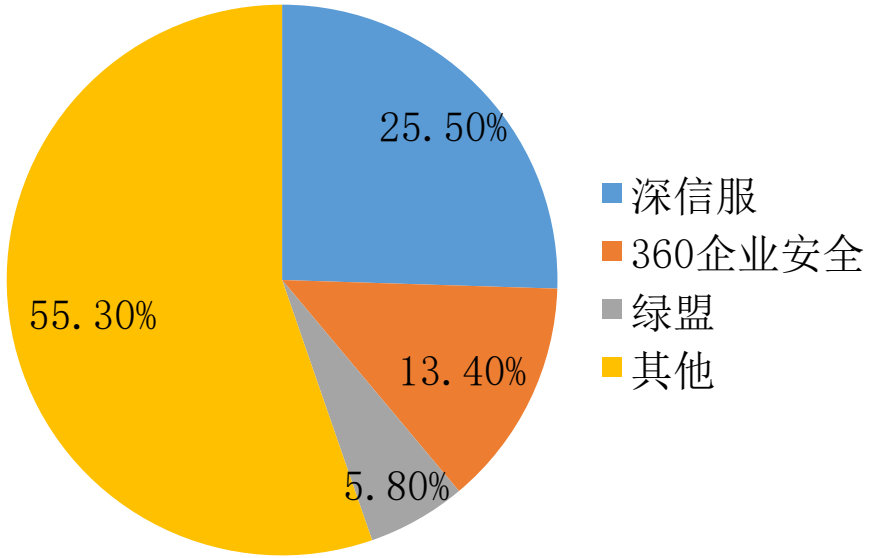
根据IDC《2018年第四季度中国IT安全硬件市场跟踪报告》，深信服在统一威胁管理硬件市场、安全内容管理硬件市场、虚拟专用网硬件市场均处于行业领先地位，启明星辰在入侵检测与防御硬件市场和虚拟专用网硬件市场拥有大量的市场份额。

图59 2018年第四季度中国统一威胁管理硬件市场份额




来源：IDC，中国银河证券研究院整理

图60 2018年第四季度中国安全内容管理硬件市场份额



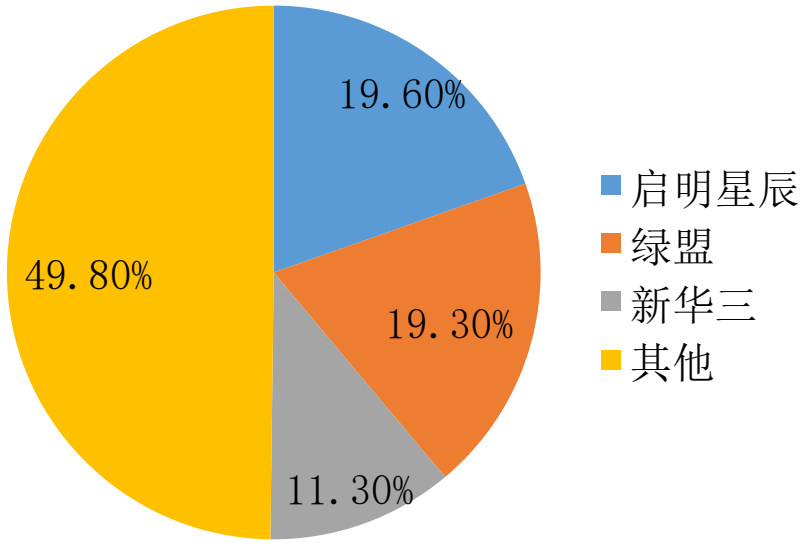

来源：IDC，中国银河证券研究院整理

# 4. 标的推荐

## 4.1 国内网络安全市场份额概况

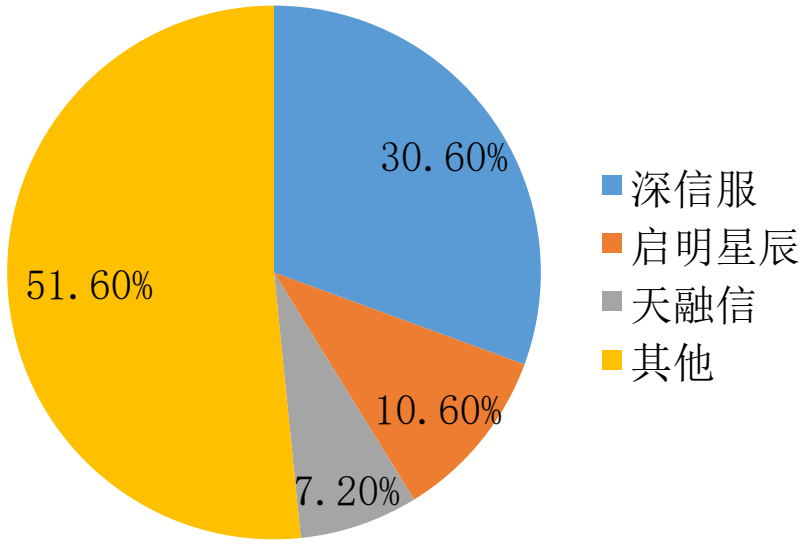
根据IDC《2018年第四季度中国IT安全硬件市场跟踪报告》，深信服在统一威胁管理硬件市场、安全内容管理硬件市场、虚拟专用网硬件市场均处于行业领先地位，启明星辰在入侵检测与防御硬件市场和虚拟专用网硬件市场拥有大量的市场份额。

图61 2018年第四季度中国入侵检测与防御硬件市场份额




来源：IDC，中国银河证券研究院整理

图62 2018年第四季度中国虚拟专用网硬件市场份额



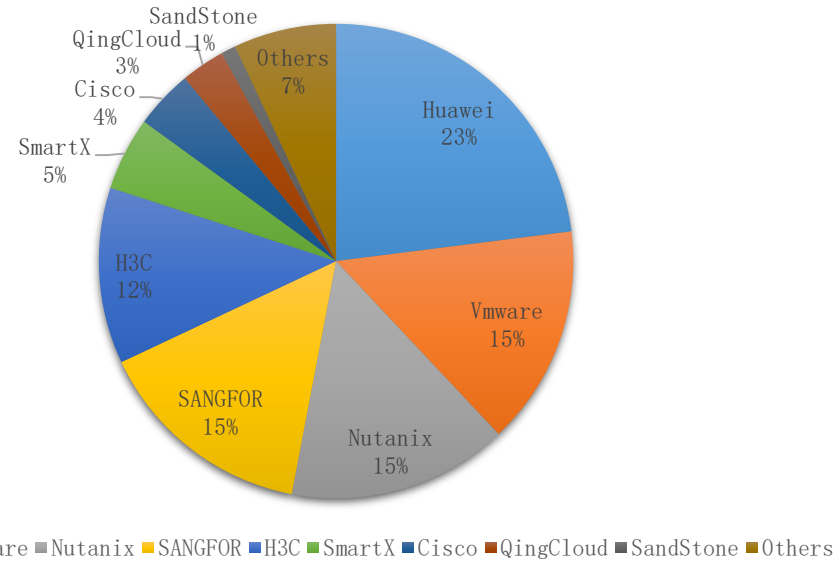

来源：IDC，中国银河证券研究院整理

# 4. 标的推荐

## 4.2 深信服

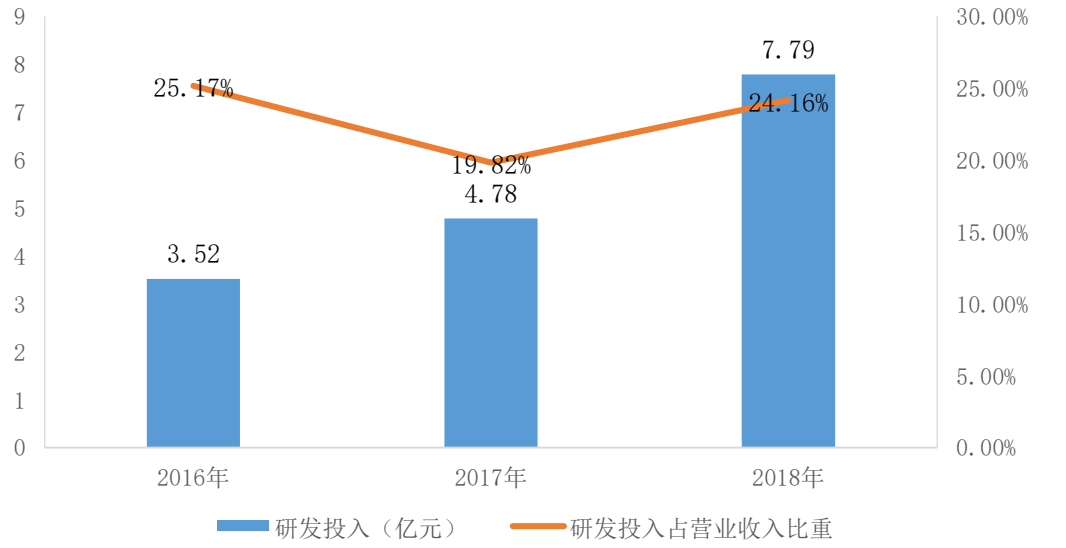
- **业绩增长稳健。**其中，网络安全和云业务持续保持高增长 。截至2018年，网络安全业务收入18.92亿，同比增长24.55%；云业务收入8.67亿，同比增长59.17%。
- **产品市场认可度高。**在软件方面，深信服占据上网行为管理市场份额25.53%，连续十年蝉联市场份额第一。2018年H1深信服超融合整体市场软件和硬件占有率为12%，排名前三；超融合软件市场占有率为15%，与Nutanix、VMware并列排名第二，超融合软件业绩增长率为233%，排名第一。
- **高研发夯实产品竞争力，前瞻性为未来业绩保驾护航。**截至2018年，公司研发投入占收入比重24.16%，远高于行业平均水平，我们认为，高研发有助于产品竞争力的可持续提升，除此之外，企业在很多新兴安全产品如云平台等上均有部署，具有较好的前瞻性，看好其未来发展。
- **公司积极拓展海外市场，战略紧跟市场趋势。**公司积极部署东南亚、中东和欧洲等市场，多元化有助于优化收入结构。

图63 2018年H1中国超融合市场份额




来源：Wind，中国银河证券研究院整理

图64 2016-2018年公司研发投入以及所占比重




来源：Wind，中国银河证券研究院整理

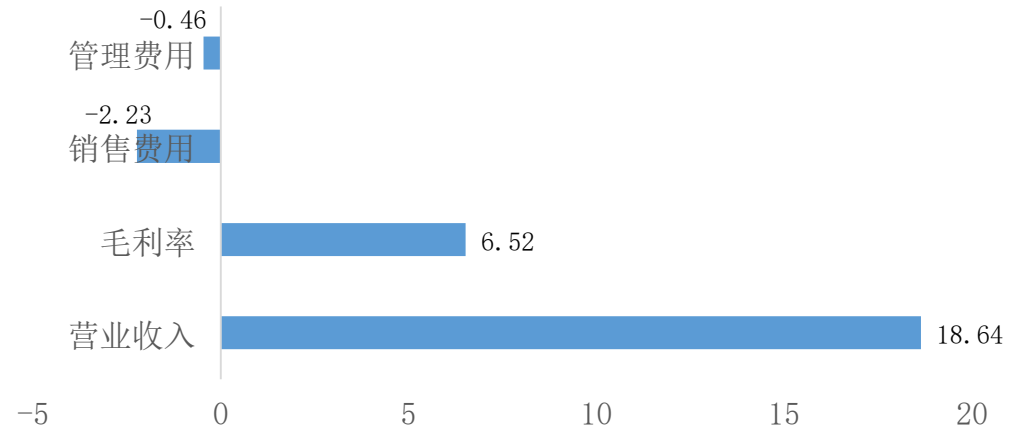
# 4. 标的推荐



## 4.3 启明星辰

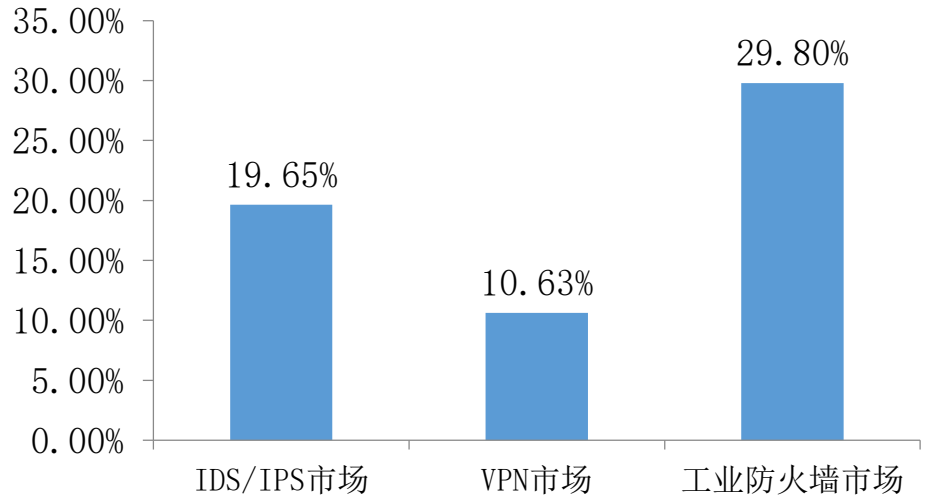
- **国内安全龙头之一。**启明星辰在信息安全行业总体市占率为8%，排名第一。根据IDC发布的2018年中国IT安全硬件市场份额统计报告：在IDS/IPS市场，启明星辰以19.65%的份额居首；VPN市场，启明星辰以10.63%的份额排名第二。新业务方面，集团以启明星辰&网御星云双品牌工业防火墙（IFW）在中国以29.8%的市场占有率领跑。
- **业绩稳健增长。**公司2019年一季度营业收入同比增长18.64%。
- **新业务工控安全、云安全符合市场发展趋势。**

图65 公司业绩表现




来源：Wind，中国银河证券研究院整理

图66 启明星辰高份额市场占比




来源：IDC，中国银河证券研究院整理

# 4. 标的推荐

## 4.4 风险提示

- 1、政策落地不及预期的风险。
- 2、新产品、新业务推广不达预期的风险。
- 3、行业竞争加剧的风险。
- 4、运营管理流失的风险。
- 5、产品销售季节性动荡的风险。
- 6、中美贸易摩擦的风险。

# 评级标准

**银河证券行业评级体系：推荐、谨慎推荐、中性、回避**
推荐：是指未来6 - 12个月，行业指数（或分析师团队所覆盖公司组成的行业指数）超越交易所指数（或市场中主要的指数）平均回报20%及以上。该评级由分析师给出。
谨慎推荐：行业指数（或分析师团队所覆盖公司组成的行业指数）超越交易所指数（或市场中主要的指数）平均回报。该评级由分析师给出。
中性：行业指数（或分析师团队所覆盖公司组成的行业指数）与交易所指数（或市场中主要的指数）平均回报相当。该评级由分析师给出。
回避：行业指数（或分析师团队所覆盖公司组成的行业指数）低于交易所指数（或市场中主要的指数）平均回报10%及以上。该评级由分析师给出。

**银河证券公司评级体系：推荐、谨慎推荐、中性、回避**
推荐：是指未来6 - 12个月，公司股价超越分析师（或分析师团队）所覆盖股票平均回报20%及以上。该评级由分析师给出。
谨慎推荐：是指未来6 - 12个月，公司股价超越分析师（或分析师团队）所覆盖股票平均回报10% - 20%。该评级由分析师给出。
中性：是指未来6 - 12个月，公司股价与分析师（或分析师团队）所覆盖股票平均回报相当。该评级由分析师给出。
回避：是指未来6 - 12个月，公司股价低于分析师（或分析师团队）所覆盖股票平均回报10%及以上。该评级由分析师给出。

**钱劲宇，计算机行业分析师。**本人具有中国证券业协会授予的证券投资咨询执业资格并注册为证券分析师，本人承诺，以勤勉的职业态度，独立、客观地出具本报告。本报告清晰准确地反映本人的研究观点。本人不曾因，不因，也将不会因本报告中的具体推荐意见或观点而直接或间接受到任何形式的补偿。本人承诺不利用自己的身份、地位和执业过程中所掌握的信息为自己或他人谋取私利。

# 免责声明

本报告由中国银河证券股份有限公司（以下简称银河证券，银河证券已具备中国证监会批复的证券投资咨询业务资格）向其机构或个人客户（以下简称客户）提供，无意针对或打算违反任何地区、国家、城市或其它法律管辖区域内的法律法规。除非另有说明，所有本报告的版权属于银河证券。未经银河证券事先书面授权许可，任何机构或个人不得更改或以任何方式发送、传播或复印本报告。

本报告所载的全部内容只提供给客户做参考之用，并不构成对客户的投资建议，并非作为买卖、认购证券或其它金融工具的邀请或保证。银河证券认为本报告所载内容及观点客观公正，但不担保其内容的准确性或完整性。客户不应单纯依靠本报告而取代个人的独立判断。本报告所载内容反映的是银河证券在最初发表本报告日期当日的判断，银河证券可发出其它与本报告所载内容不一致或有不同结论的报告，但银河证券没有义务和责任去及时更新本报告涉及的内容并通知客户。银河证券不对因客户使用本报告而导致的损失负任何责任。

银河证券不需要采取任何行动以确保本报告涉及的内容适合于客户。银河证券建议客户如有任何疑问应当咨询证券投资顾问并独自进行投资判断。本报告并不构成投资、法律、会计或税务建议或担保任何内容适合客户，本报告不构成给予客户个人咨询建议。

本报告可能附带其它网站的地址或超级链接，对于可能涉及的银河证券网站以外的地址或超级链接，银河证券不对其内容负责。本报告提供这些地址或超级链接的目的纯粹是为了客户使用方便，链接网站的内容不构成本报告的任何部份，客户需自行承担浏览这些网站的费用或风险。

银河证券在法律允许的情况下可参与、投资或持有本报告涉及的证券或进行证券交易，或向本报告涉及的公司提供或争取提供包括投资银行业务在内的服务或业务支持。银河证券可能与本报告涉及的公司之间存在业务关系，并无需事先或在获得业务关系后通知客户。

银河证券无需因接收人收到本报告而视其为客户。本报告是发送给银河证券客户的，属于机密材料，只有银河证券客户才能参考或使用，如接收人并非银河证券客户，请及时退回并删除。



**联系**

**中国银河证券股份有限公司 研究院**

**深圳市福田区福华一路中心商务大厦26层**

**上海浦东新区富城路99号震旦大厦31层**

**北京市西城区金融街35号国际企业大厦C座**

**公司网址：www.chinastock.com.cn**

机构请致电：

深广地区：崔香兰 0755-83471963 cuixinglan@chinastock.com.cn

上海地区：何婷婷 021-20252612 hetingting@chinastock.com.cn

北京地区：耿尤繇 010-66568479 gengyouyou@chinastock.com.cn