

从北京网络安全大会（BCS）看网络安全发展趋势

2019年8月21日至8月23日，网络安全行业的“达沃斯”——2019北京网络安全大会（BCS 2019）在北京国家会议中心召开。本次会议由中国电子信息产业集团主导，中国互联网协会、中国网络空间安全协会、中国通信学会、中国友谊促进会和奇安信集团承办，齐聚了20位两院院士，与来自30多个国家、70多所全球知名院校、机构和企业的400多位国内外安全领袖，共同探讨网络安全行业的前沿问题。本报告将结合此次BCS会议的内容对我国网络安全行业的发展趋势探究一二。

核心观点

- 《网络安全法》规定实行网络安全等级保护，并强调对关键信息基础设施实行重点保护，网络安全等级保护制度2.0标准已正式发布，并于年底实施，届时将刺激网络安全需求进一步释放。当前各省的等保宣贯会也在如火如荼展开，拥有第三级及以上的信息系统的政府、金融、电信等领域势必会加大信息安全投入，以符合等保2.0的规范和要求，安全厂商也纷纷将等保建设作为自身业务拓展的重点。
- 新兴安全领域成为众多厂商的布局重点。随着大数据、云计算、移动互联网、物联网等新兴产业发展，企业的核心业务越发依托信息系统，这带来了新的问题，云安全、数据安全、工控安全等新兴安全领域应运而生且保持高速发展，吸引众多安全厂商进行布局。
- 随着等保2.0即将落地实施，信息安全已成为企业或组织的重要工作，安全运营的重要性凸显。同时，物联网、云计算等技术的普及使得安全运营的范围和边界急速扩张，再加上网络安全人才缺口严重，当前企业自身安全运营体系也存在诸多痛点。当下态势感知等主动防御产品的逐渐成熟成为优质安全运营服务的重要支撑，面临着安全运营服务的巨大需求，许多厂商也纷纷加入赛道，推出自身的安全运营平台和解决方案。

投资建议

- 目前我国传统信息安全产品市场已经成熟，竞争格局趋于稳定，信息安全头部企业均有自己优势的细分市场，并存在一定的壁垒，这使得企业扩大信息安全产品市场份额变得不易。我们认为未来两类信息安全公司具备快速成长机会，建议关注：1) 立足信息安全良好赛道，并在其他行业拥有强劲增长点的信息安全公司，如多款安全产品市占率领先同时在云计算领域深耕的深信服(300454, 增持)、电子数据取证龙头同时大数据信息化业务快速增长的美亚柏科(300188, 未评级)；2) 提前布局云安全、工控安全等新兴安全领域，以及商业模式有所突破的信息安全公司，如在工控安全等新兴领域布局同时安全运营服务表现突出的启明星辰(002439, 未评级)以及同样在云安全，工控安全布局并向安全解决方案+安全运营模式转化的绿盟科技(300369, 未评级)。

风险提示

- 网络安全政策落地不及预期；网络安全行业发展不及预期。

资料来源：公司数据，东方证券研究所预测，每股收益使用最新股本全面摊薄计算，（上表中预测结论均取自最新发布上市公司研究报告，可能未完全反映该上市公司研究报告发布之后发生的股本变化等因素，敬请注意，如有需要可参阅对应上市公司研究报告）

东方证券股份有限公司经相关主管机关核准具备证券投资咨询业务资格，据此开展发布证券研究报告业务。

东方证券股份有限公司及其关联机构在法律许可的范围内正在或将要与本研究报告所分析的企业发展业务关系。因此，投资者应当考虑到本公司可能存在对报告的客观性产生影响的利益冲突，不应视本证券研究报告为作出投资决策的唯一因素。

有关分析师的申明，见本报告最后部分。其他重要信息披露见分析师申明之后部分，或请与您的投资代表联系。并请阅读本证券研究报告最后一页的免责声明。

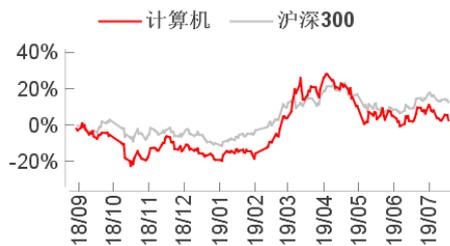


东方证券
ORIENT SECURITIES

行业评级 看好 中性 看淡 (维持)

国家/地区 中国
行业 计算机行业
报告发布日期 2019年08月29日

行业表现



资料来源：WIND、东方证券研究所

证券分析师 浦俊懿
021-63325888*6106
pujunyi@orientsec.com.cn
执业证书编号：S0860514050004

证券分析师 游涌洋
010-66210783
youjuanyang@orientsec.com.cn
执业证书编号：S0860515080001

联系人 陈超
021-63325888-3144
chenchao3@orientsec.com.cn

相关报告

科创板受理信息安全公司一览： 2019-08-25
信息安全行业科创板公司：安恒信息： 2019-07-08

目 录

| | |
|------------------------------------|----|
| 一、BCS 大会概览..... | 4 |
| 二、关键信息基础设施安全保护与等保 2.0 政策备受关注 | 5 |
| 三、新兴安全领域成为重点厂商的布局重点 | 8 |
| 3.1 新兴技术带来新的安全风险 | 8 |
| 3.2 云安全 | 9 |
| 3.3 数据安全..... | 10 |
| 3.4 工控安全..... | 11 |
| 3.5 电子数据取证 | 13 |
| 四、安全服务正在发生从运维走向运营的深刻变革 | 13 |
| 投资建议..... | 15 |
| 风险提示..... | 16 |

图表目录

| | |
|--------------------------------|----|
| 图 1: 2019 BCS 参展企业一览 | 4 |
| 图 2: BCS 各分论坛主题 | 5 |
| 图 3: 关键信息基础设施 | 6 |
| 图 4: 我国等级保护发展历程 | 6 |
| 图 5: 等保 2.0 标准体系 | 7 |
| 图 6: 等保 2.0 主要标准 | 7 |
| 图 7: 信息安全的价值量不断提升 | 8 |
| 图 8: 新技术对安全的影响 | 9 |
| 图 9: 我国公有云市场规模及增速（亿元，%） | 9 |
| 图 10: 我国私有云市场规模及增速（亿元，%） | 9 |
| 图 11: 云计算面临更多的安全风险 | 10 |
| 图 12: 光通天下云安全产品 | 10 |
| 图 13: 安全狗云安全产品矩阵 | 10 |
| 图 14: 网络攻击的首要目标占比 | 11 |
| 图 15: 闪捷信息云管端立体化数据安全解决方案 | 11 |
| 图 16: 工控系统安全面临诸多痛点 | 12 |
| 图 17: 奇安信工业安全监测系统及控制平台 | 12 |
| 图 18: 奇安信盘古石取证产品及服务 | 13 |
| 图 19: 企业安全运营体系三大挑战 | 14 |
| 图 20: 安全进化论——滑动标尺模型 | 14 |
| 图 21: 奇安信态势感知与安全运营平台 | 15 |

图 2：BCS 各分论坛主题



数据来源：BCS 官网，东方证券研究所

二、关键信息基础设施安全保护与等保 2.0 政策备受关注

《网络安全法》规定实行网络安全等级保护，并强调对关键信息基础设施实行重点保护。《网络安全法》第二十一条规定：国家实行网络安全等级保护制度。第三十一条规定：国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。本届 BCS 大会对于关键信息基础设施保护与网络安全等级保护展开了深入讨论，吸引力众多观众前来参会。

图 3：关键信息基础设施



数据来源：新华网，东方证券研究所

网络安全等级保护是指对国家重要信息、法人和公民等的专有信息、公开信息，以及存储、传输、处理上述信息的信息系统等级实行安全保护，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，其发展历程已有 20 余年。随着云计算、物联网等新技术的发展，网络安全态势越发复杂，等保 1.0 标准已不适用，等保体系升级是必然选择。升级后的等保 2.0 体系根据信息技术的发展和网络安全的态势，不断丰富等保内容和保护范围。

图 4：我国等级保护发展历程

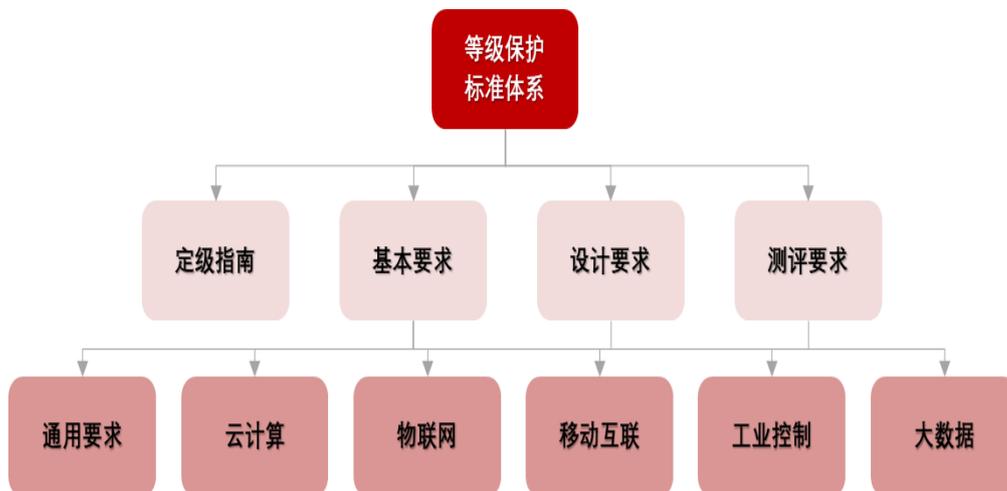


数据来源：互联网，东方证券研究所

《网络安全法》和《网络安全等级保护条例》为等保 2.0 提供了制度保障，使得网络安全等级保护上升为法律，网络安全行业走向合规性与强制性驱动并重的阶段。等级保护工作的主要流程包括定级、备案、建设整改、等级测评、安全自查与监督检查五个规定动作，其标准体系横向扩展了对云

计算、移动互联网、物联网、工业控制系统、大数据的安全要求，纵向扩展了对等保测评机构的规范管理。

图 5：等保 2.0 标准体系



数据来源：互联网，东方证券研究所

2019 年 5 月，部分网络安全等级保护制度 2.0 标准正式发布，但标准体系中定级智能及实施指南的标准仍在制定中，预计近期会正式发布。标准将于 2019 年 12 月 1 日开始正式实施，各省的等保宣贯会也在如火如荼展开，我们认为等保 2.0 在正式出台后，拥有第三级及以上的信息系统的政府、金融、电信等领域势必会加大信息安全投入，以符合等保 2.0 的规范和要求，这将带动网络安全市场规模提速增长。

图 6：等保 2.0 主要标准

网络安全等级保护 2.0-主要标准

- 计算机信息系统安全保护等级划分准则 (GB 17859-1999)
- 网络安全等级保护定级指南 (GB/T22240) (待发布)
- 网络安全等级保护基本要求 (GB/T22239-2019)
- 网络安全等级保护设计技术要求 (GB/T25070-2019)
- 网络安全等级保护测评要求 (GB/T28448-2019)
- 网络安全等级保护测评过程指南 (GB/T28449-2018)
- 网络安全等级保护实施指南 (GB/T25058) (待发布)

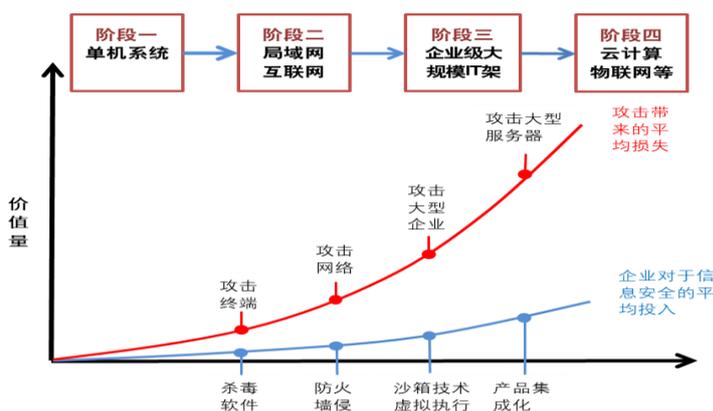
数据来源：BCS，东方证券研究所

三、新兴安全领域成为重点厂商的布局重点

3.1 新兴技术带来新的安全风险

“云大物移智”等新技术的出现，信息安全的价值量不断上升。信息安全并不能直接创造价值，信息安全的价值量由信息系统本身的价值决定，而随着云计算、大数据、物联网、移动互联网、人工智能等新技术的出现与发展，信息系统及其承载的业务及数据的价值大大提升，这使得每次遭遇网络攻击造成的平均损失不断提高，对于信息系统及其承载的业务及数据的防护也变得越发必要，因此企业也随之加大对信息安全的投入。

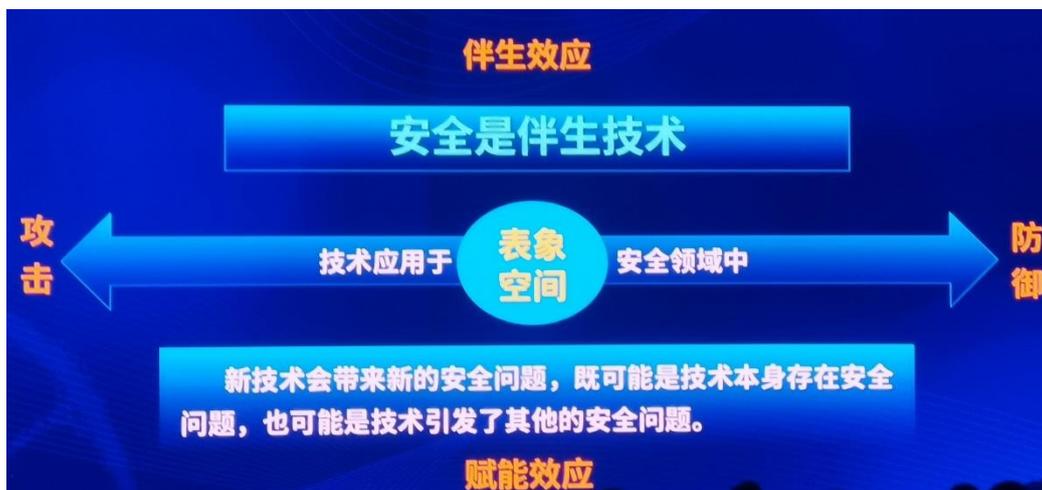
图 7：信息安全的价值量不断提升



数据来源：智研咨询，东方证券研究所

网络安全的本质在于攻防两端的对抗，云计算、大数据、5G 等新技术的出现既能助长攻击也能助长防御，同时也会带来新的安全问题。当新技术应用于安全领域中，对于攻击方来说，新兴技术可以为其攻击手段赋能，如云计算平台可被用作 DdoS 攻击平台，会使 DdoS 攻击显著增强，但对于防御方来说，同样也能产生正面的赋能效应，如通过云平台进行大规模病毒查杀工作，以替代较为低效的终端杀毒行为。另一方面，新兴技术的应用自身也会带来安全问题，一是技术本身的脆弱性会伴生新的安全问题，如大数据在交易时可能会被买家二次授权从而侵犯卖家的利益，二是新技术可能让其他事务变得不安全，如大数据可以通过统计分析等手段挖掘用户隐私，带来隐私安全问题。

图 8：新技术对安全的影响

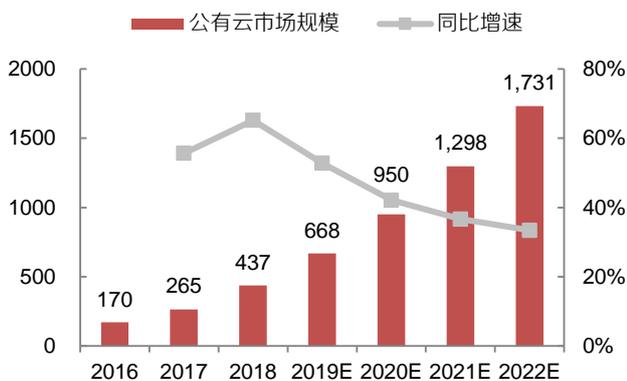


数据来源：BCS，东方证券研究所

3.2 云安全

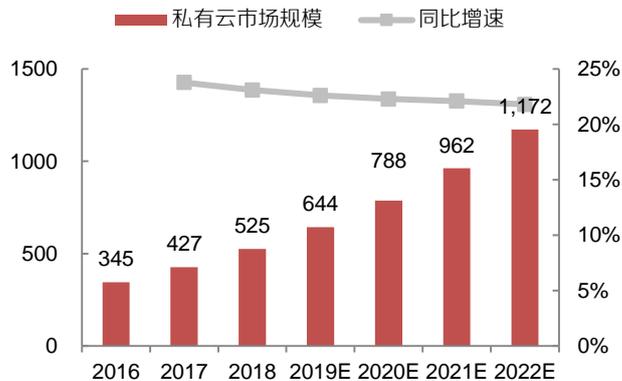
当前我国云计算产业仍处于高速增长阶段。中国信息通信研究院数据显示，2018 年我国公有云市场规模达到 437 亿元，预计 2018-2022 年 CAGR 达到 41%，我国私有云市场规模达到 427 亿元，预计 2018-2022 年 CAGR 达到 22%，低于公有云增速。当前我国云计算市场规模在全球总市场的占比较小，仍有巨大的发展空间，未来有望继续保持高速增长。

图 9：我国公有云市场规模及增速（亿元，%）



数据来源：中国信息通信研究院，东方证券研究所

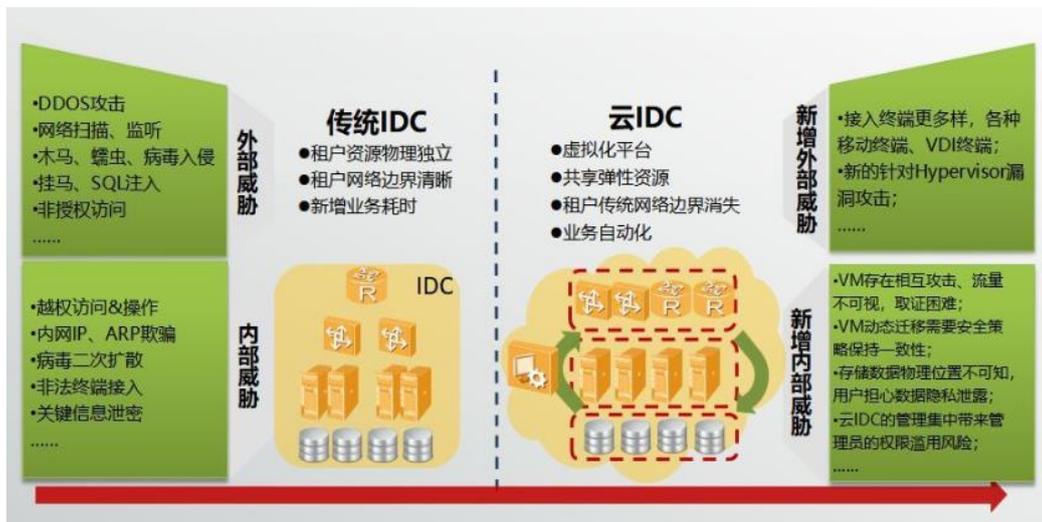
图 10：我国私有云市场规模及增速（亿元，%）



数据来源：中国信息通信研究院,东方证券研究所

云计算使得 IT 基础架构发生根本性变化，并带来新的安全风险。云计算环境下服务器、存储、网络等虚拟化技术为云服务提供了基础技术支持，并解决了资源利用率及资源提供的自动扩展等问题，但也使得传统安全边界概念消失。另外，企业将其业务迁移到云端，云计算的服务配置和业务规模都可根据用户的需求进行灵活配置，IT 基础资源向云端集中，这些都使得云计算相较于传统 IT 架构面临更多的安全风险。

图 11：云计算面临更多的安全风险



数据来源：CSDN，东方证券研究所

本次大会参展厂商中有众多云安全厂商，包括奇安信、光通天下（已申报科创板）、白山云科技（已申报科创板）、安全狗（美亚柏科参股公司）、青松云安全等公司。其中光通天下提供的云安全产品及服务包括睿盾抗 DdoS 云防护平台、智能 WAF 服务、智能 CC 防护服务、渗透测试服务以及态势感知服务，可帮助客户在最小成本的情况下获取便捷、按需、可扩展的网络安全防护服务。

图 12：光通天下云安全产品



数据来源：BCS，东方证券研究所

图 13：安全狗云安全产品矩阵

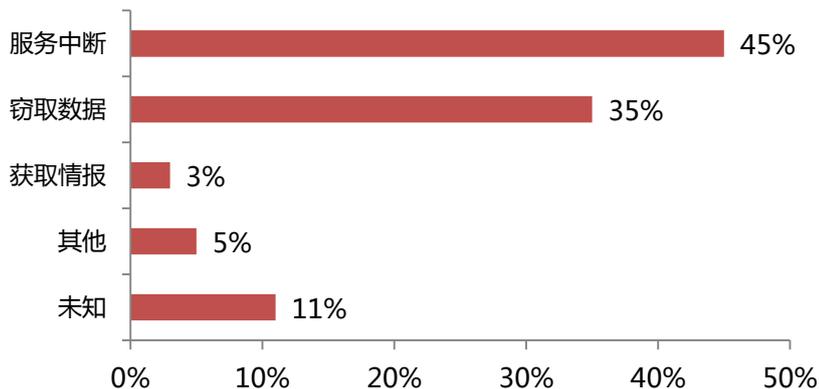


数据来源：BCS，东方证券研究所

3.3 数据安全

随着信息化建设的逐步推进，企业的核心业务越发依托信息系统，数据已成为企业的核心资产。新兴技术的不断涌现使得企业自身业务越发依赖于互联网，数据安全风险已经成为用户最为关注的安全风险之一。当前数据窃取和服务终端已成为多数网络攻击的首要目标，分别占到 35%和 45%。

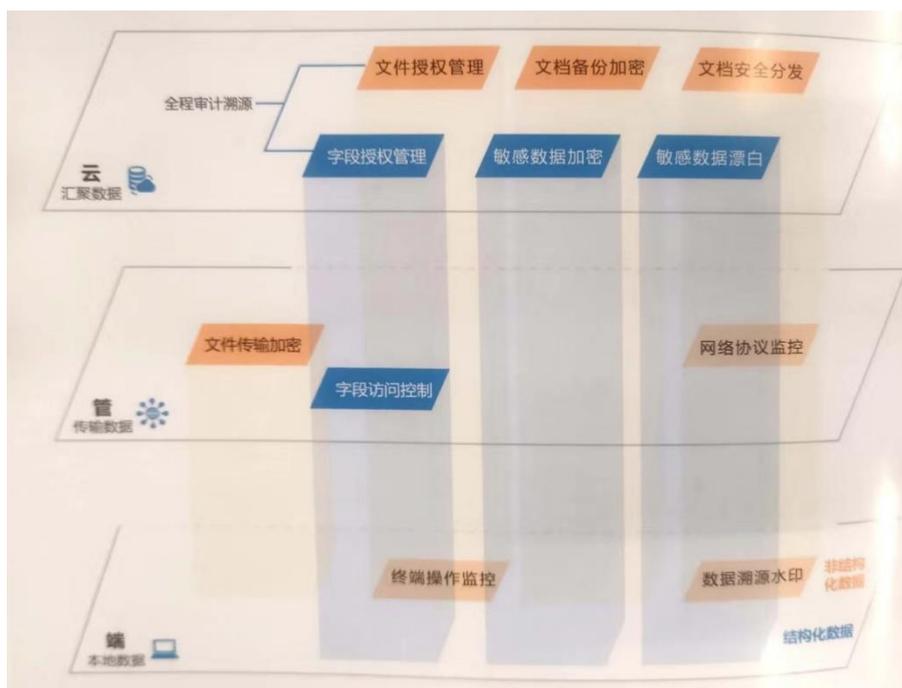
图 14：网络攻击的首要目标占比



数据来源：Radware，东方证券研究所

数据安全同样是众多安全厂商的重点业务，相关厂商包括闪捷信息、中安威士、昂楷科技等。各厂商的数据安全解决方案从数据的收集、传输、加工、存储、应用等全生命周期出发，提供数据加密、访问控制、数据脱敏等多种功能的数据防护。

图 15：闪捷信息云管端立体化数据安全解决方案



数据来源：BCS，东方证券研究所

3.4 工控安全

当前工业安全事件数量呈现逐年上升的趋势，企业所遭受的损失也在逐步扩大。根据 Gartner 调查，约 20%的企业或相关机构在近三年内至少遭受了一次基于物联网的攻击。而对工控系统的安

全防护面临诸多痛点，如对自身资产状况不清晰，对系统面临的安全威胁知之甚少，同时对系统运行的状况无法了解。

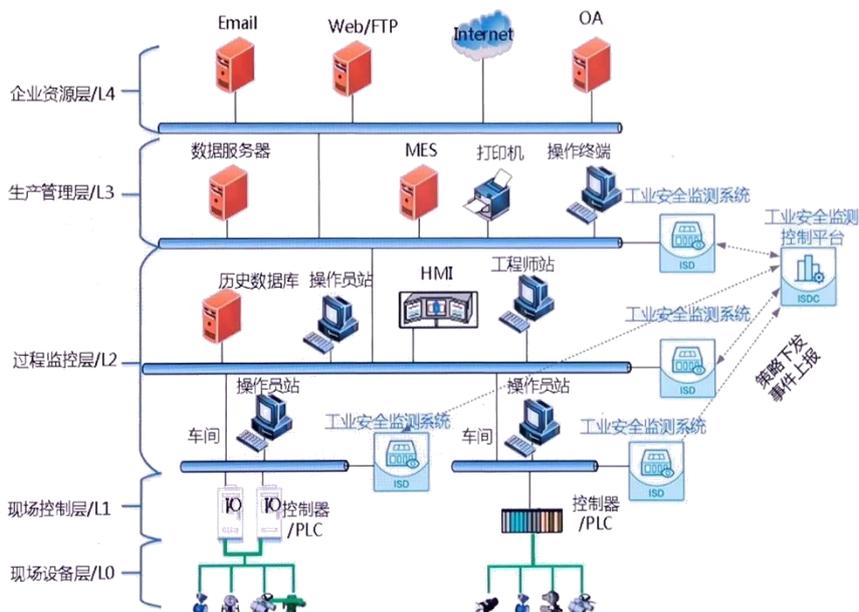
图 16: 工控系统安全面临诸多痛点



数据来源：奇安信，东方证券研究所

工控安全市场高速发展，大型安全厂商纷纷布局。随着工业互联网的快速推进，我国工控安全市场同样呈现高速发展的态势，2017 年市场规模达到 5.6 亿，预计 2019 年达到 13.1 亿，复合增速超过 50%。目前，启明星辰、中新赛克等上市公司都已布局工控安全领域，而在 BCS 大会中，奇安信也发布自己的工控安全产品。

图 17: 奇安信工业安全监测系统及控制平台



数据来源：奇安信，东方证券研究所

3.5 电子数据取证

云计算、物联网、移动互联网等新技术的发展，使得社会数据化、互联网化水平不断提升，新型电子数据取证工具应运而生，如云取证、芯片取证、IOT 取证等。同时涉及电子数据的案件越来越多，电子数据取证的需求保持长期稳定增长。短期来看，国务院政府机构改革已在今年一季度基本技术，公安各警种、税务稽查等方面的电子数据取证需求逐渐恢复，奇安信也逐渐开始布局该领域，推出自己的取证品牌“盘古石”。

图 18：奇安信盘古石取证产品及服务



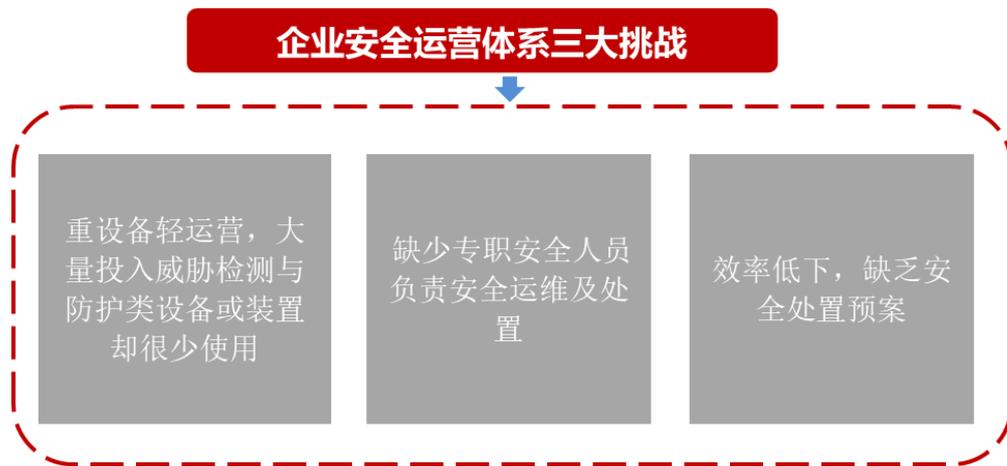
数据来源：BCS，东方证券研究所

四、安全服务正在发生从运维走向运营的深刻变革

安全运营是目前行业中普遍关注的话题，本次大会同样对安全运营展开深刻讨论。随着等保 2.0 即将落地实施，信息安全已成为企业或组织的重要工作，安全运营的重要性凸显。同时，物联网、云计算等技术的普及使得安全运营的范围和边界急速扩张，再加上网络安全人才缺口严重，当前企业自身安全运营体系也存在诸多痛点：

- 1) 重设备轻运营。大量投入威胁检测与防护类设备或装置却很少使用；
- 2) 缺少专职安全人员负责安全运维及处置；
- 3) 效率低下，缺乏安全处置预案。

图 19：企业安全运营体系三大挑战



数据来源：东方证券研究所

主动防御产品支撑安全运营能力。态势感知、威胁情报等主动防御类产品也是展会部分的重要看点，当前被动防御产品已无法满足企业业务的安全需要，而态势感知、威胁情报等主动防御产品可以在入侵行为对信息系统发生影响之前，及时精准预警，实时构建弹性防御体系，避免、转移、降低信息系统面临的风险，有效支撑安全运营服务。

图 20：安全进化论——滑动标尺模型



数据来源：奇安信，东方证券研究所

安全运营可以解决客户安全运营的痛点，提升客户的防御能力。提供安全运营服务的企业可将客户的安全业务进行集中托管，提供有效、连续（7*24 小时）的安全服务，同时也能减少企业自身去客户处的运维人员数量，降低企业成本。当前安全运营也成为了安全厂商的业务拓展方向，如启明星辰、绿盟科技、奇安信开展智慧城市安全运营、深信服开展的安全托管服务等。

图 21：奇安信态势感知与安全运营平台



数据来源：奇安信，东方证券研究所

投资建议

目前我国信息安全行业增速平稳，传统信息安全产品市场已经成熟，竞争格局趋于稳定，信息安全头部企业均有自己优势的细分市场，并存在一定的壁垒，这使得企业扩大信息安全产品市场份额变得不易。我们认为未来两类信息安全公司具备快速成长机会：

1) 立足信息安全良好赛道，并在其他行业拥有强劲增长点的信息安全公司。

- 深信服(300454, 增持): 公司多款安全产品市占率领先, 其中 VPN 产品连续七年市占率第一, VPN 应用十分广泛, 细分市场规模较大, 预计 2018 年防火墙/VPN 市场规模达到 80 亿元。同时公司拥有强大的渠道能力和研发能力, 并积极围绕等保需求布局。此外公司还提供云安全及企业级无线产品, 其中云安全业务发展迅速, 2018 年营收为 8.7 亿元, 近三年 CAGR 高达 129.2%, 超融合产品市占率已位居国内第三 (2018)。
- 美亚柏科(300188, 未评级): 电子取证行业绝对龙头, 市占率在 40%以上。电子取证行业随着新技术的发展不断拓展市场空间, 如云取证、芯片取证等, 并在下游行业维度和区域维度不断纵深。随着机构改革完成, 电子数据取证需求有望放量。此外, 公司深耕大数据信息化业务, 营收从 2015 年的 0.46 亿增长到 2018 年的 4.96 亿, CAGR 达到 121%。

2) 提前布局云安全、工控安全等新兴安全领域, 以及商业模式有所突破的信息安全公司

- 启明星辰(002439, 未评级): 通过内生外延, 覆盖数据安全、云安全、工控安全等新兴领域, 公司安全产品线十分完善, UTM、IDS/IPS 产品等多款产品保持市占率第一。公司积极拓展智慧城市安全运营服务, 实现商业模式的升级, 已初见成效。2018 年已在 20 个城市开展相关业务, 公司 2019 年计划建设数量累加达到 35 个以上。

- 绿盟科技(300369, 未评级): 公司持续推进 P2SO 战略, 即向安全解决方案+安全运营模式转化, 目前公司在工控安全、云安全等领域都取得不错的进展, 并在智慧城市安全运营、行业联合安全运营及企业安全运营商发力, 在中国电科产业基金入股后, 公司积极拓展政府市场业务, 上半年收入及业绩明显改善。

风险提示

1、网络安全政策落地不及预期

政策是驱动信息安全快速发展的重要力量, 若相关政策落地不及预期, 导致行业需求出现波动, 对行业内相关公司的经营造成不利影响。

2、网络安全行业发展不及预期

若云计算、物联网等新兴产业发展不及预期, 会影响网络安全的需求, 从而对网络安全整体行业的发展带来负面影响。

分析师申明

每位负责撰写本研究报告全部或部分内容的研究分析师在此作以下声明：

分析师在本报告中对所提及的证券或发行人发表的任何建议和观点均准确地反映了其个人对该证券或发行人的看法和判断；分析师薪酬的任何组成部分无论是在过去、现在及将来，均与其在本研究报告中所表述的具体建议或观点无任何直接或间接的关系。

投资评级和相关定义

报告发布日后的 12 个月内的公司的涨跌幅相对同期的上证指数/深证成指的涨跌幅为基准；

公司投资评级的量化标准

买入：相对强于市场基准指数收益率 15%以上；

增持：相对强于市场基准指数收益率 5% ~ 15%；

中性：相对于市场基准指数收益率在-5% ~ +5%之间波动；

减持：相对弱于市场基准指数收益率在-5%以下。

未评级 —— 由于在报告发出之时该股票不在本公司研究覆盖范围内，分析师基于当时对该股票的研究状况，未给予投资评级相关信息。

暂停评级 —— 根据监管制度及本公司相关规定，研究报告发布之时该投资对象可能与本公司存在潜在的利益冲突情形；亦或是研究报告发布当时该股票的价值和价格分析存在重大不确定性，缺乏足够的研究依据支持分析师给出明确投资评级；分析师在上述情况下暂停对该股票给予投资评级等信息，投资者需要注意在此报告发布之前曾给予该股票的投资评级、盈利预测及目标价格等信息不再有效。

行业投资评级的量化标准：

看好：相对强于市场基准指数收益率 5%以上；

中性：相对于市场基准指数收益率在-5% ~ +5%之间波动；

看淡：相对于市场基准指数收益率在-5%以下。

未评级：由于在报告发出之时该行业不在本公司研究覆盖范围内，分析师基于当时对该行业的研究状况，未给予投资评级等相关信息。

暂停评级：由于研究报告发布当时该行业的投资价值分析存在重大不确定性，缺乏足够的研究依据支持分析师给出明确行业投资评级；分析师在上述情况下暂停对该行业给予投资评级信息，投资者需要注意在此报告发布之前曾给予该行业的投资评级信息不再有效。

免责声明

本证券研究报告（以下简称“本报告”）由东方证券股份有限公司（以下简称“本公司”）制作及发布。

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本公司的当然客户。本报告的全体接收人应当采取必要措施防止本报告被转发给他人。

本报告是基于本公司认为可靠的且目前已公开的信息撰写，本公司力求但不保证该信息的准确性和完整性，客户也不应该认为该信息是准确和完整的。同时，本公司不保证文中观点或陈述不会发生任何变更，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证券研究报告。本公司会适时更新我们的研究，但可能会因某些规定而无法做到。除了一些定期出版的证券研究报告之外，绝大多数证券研究报告是在分析师认为适当的时候不定期地发布。

在任何情况下，本报告中的信息或所表述的意见并不构成对任何人的投资建议，也没有考虑到个别客户特殊的投资目标、财务状况或需求。客户应考虑本报告中的任何意见或建议是否符合其特定状况，若有必要应寻求专家意见。本报告所载的资料、工具、意见及推测只提供给客户作参考之用，并非作为或被视为出售或购买证券或其他投资标的的邀请或向人作出邀请。

本报告中提及的投资价格和价值以及这些投资带来的收入可能会波动。过去的表现并不代表未来的表现，未来的回报也无法保证，投资者可能会损失本金。外汇汇率波动有可能对某些投资的价值或价格或来自这一投资的收入产生不良影响。那些涉及期货、期权及其它衍生工具的交易，因其包括重大的市场风险，因此并不适合所有投资者。

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，投资者自主作出投资决策并自行承担投资风险，任何形式的分享证券投资收益或者分担证券投资损失的书面或口头承诺均为无效。

本报告主要以电子版形式分发，间或也会辅以印刷品形式分发，所有报告版权均归本公司所有。未经本公司事先书面协议授权，任何机构或个人不得以任何形式复制、转发或公开传播本报告的全部或部分内容。不得将报告内容作为诉讼、仲裁、传媒所引用之证明或依据，不得用于营利或用于未经允许的其它用途。

经本公司事先书面协议授权刊载或转发的，被授权机构承担相关刊载或者转发责任。不得对本报告进行任何有悖原意的引用、删节和修改。

提示客户及公众投资者慎重使用未经授权刊载或者转发的本公司证券研究报告，慎重使用公众媒体刊载的证券研究报告。

东方证券研究所

地址：上海市中山南路 318 号东方国际金融广场 26 楼

联系人：王骏飞

电话：021-63325888*1131

传真：021-63326786

网址：www.dfzq.com.cn

Email：wangjunfei@orientsec.com.cn

