中信证券 CITIC SECURITIES

科技先锋系列报告93

Check Point：全球领先的网络安全厂商

许英博 首席科技产业分析师

陈俊云 前瞻研究高级分析师

中信证券研究部·前瞻研究

2020年6月4日

图片来源：Check Point官网

Check Point：全球网络安全先驱

- Check Point Software Technologies Ltd.是面向全球企业和政府提供网络安全解决方案的领先供应商。其解决方案对恶意软件、勒索软件和其他针对性攻击的捕获率均为业界领先，可保护客户免受第五代网络攻击威胁。
- Check Point将第五代高级威胁防护与业界先进的单点控制管理系统相结合，提供多层的安全架构，保护企业网络、云端和移动业务免受已知攻击。

Check Point发展历程

1993 由Gil Shwed于1993年在以色列创立，推出FireWall-1，这是IT业的第一种状态检测防火墙技术

1996 在纳斯达克上市

2006 通过使用单个管理控制台，统一安全网关和第一个基于代理的端点保护创建统一安全体系结构UTM

2009 推出刀片软件架构，可以为企业定制安全、灵活和简单的解决方案

2012 推出防御网络犯罪的协同式网络ThreatCloud；推出虚拟系统简化私有云安全

2014 推出移动安全解决方案Check Point Capsule

2017 推出了Check Point Infinity，提供跨网络、云，端点和移动的首个整合安全保护

2018 推出了针对第五代网络威胁的Gen V防护体系

资料来源：Check Point官网，IT168，中信证券研究部

网络安全产品

- Check Point网络安全产品线致力于为各种规模组织提供最新的数据和网络安全防护，能保护用户免受第五代与零日网络攻击，并降低复杂性和总体拥有成本。
  - SandBlast Network 是一套完善的网络威胁防护解决方案，可以运用威胁仿真与 CPU 级检查捕获恶意软件，通过威胁剥离功能消除潜在威胁，提供无风险环境以保障用户业务流程的连续性。
  - 下一代防火墙 (NGFW) 打造完善的防护技术，包括反勒索软件和 CPU 级仿真能力，提供跨所有网络分段的最具创新性和有效性的安全防护。
  - 安全网关设备从小规模威胁到第五代大规模攻击，均可提供威胁防护和统一的安全管理。

网络安全产品系列

高级威胁防护

Check Point SandBlast 提供业界领先的网络防护，哪怕最复杂的恶意软件和零日威胁也能轻松抵御。

下一代防火墙

下一代威胁防护软件为各种规模的组织提供了对已知与未知威胁的全面防护。

安全网关设备

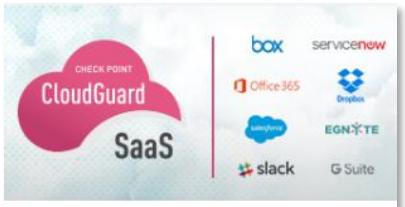
Check Point 安全网关为您提供针对任何网络攻击的全面性威胁防护。

资料来源：Check Point官网

云安全产品

- 借助动态可扩展性、智能配置功能及贯穿物理和虚拟网络的一致控制，Check Point云安全解决方案可为云中资产防御复杂威胁：
  - Check Point CloudGuard SaaS通过防止对于 SaaS 应用程序和云端电子邮件的针对性攻击来保护企业数据。
  - CloudGuard 公有云安全IaaS提供自动化、灵活性的公有云网络安全防护保护资产及数据，同时与公共云环境的动态需求保持一致；私有云安全IaaS在虚拟数据中心提供动态私有云安全，防止威胁的横向传播，同时加强跨物理和虚拟网络的可见性及管理。
  - CloudGuard Dome9 是一个用于公有云安全及合规编排的综合软件平台。

云安全产品系列



SaaS 安全

CloudGuard SaaS 针对未知威胁、未知恶意软件和零日攻击，为 SaaS 用户带来主动性的安全防护。

公有云安全IaaS

CloudGuard IaaS 可实现与公有云资产的可靠连接，同时通过跨公有云和混合云环境的高级威胁防护来保护应用程序与数据。

私有云安全IaaS

CloudGuard IaaS 可提供无缝的高级威胁防护，以防止威胁的传播，同时实现对物理和虚拟环境的可见性与控制

CloudGuard Dome9

CloudGuard Dome9 可在公有云 (AWS、Azure、GCP) 中提供可见性、持续合规、主动防护与威胁检测

资料来源：Check Point官网

移动安全产品

- Check Point企业移动终端安全解决方案帮助用户保护业务数据，为移动设备提供对业务文档的安全访问，并使移动设备免受威胁。
  - SandBlast Mobile是领先的企业移动终端安全和移动威胁防御（MTD）解决方案，提供高级防护、高捕获率和全面的威胁可见性。
  - Capsule移动终端安全工作区是一个移动设备安全内容存放区，它能在个人设备上创建独立的公司工作区域，对公司网络内外的公司数据及资产进行保护。

移动安全产品系列

移动威胁防御

Check Point 的 SandBlast Mobile 保护 iOS 和 Android 设备免受高级移动威胁的攻击，让您可以放心部署和保护设备。

移动终端安全工作区

Capsule Workspace 为移动设备的使用提供了一个安全的业务环境，并可随时随地保护业务文档。

资料来源：Check Point官网

终端安全产品

- Check Point终端安全产品通过数据安全、网络安全、威胁防护及VPN远程访问为Windows 和 Mac OS X 提供完整安全性的单独代理。终端安全作为集成套件，为用户提供了简单、统一的管理流程及策略实施。
  - SandBlast Agent是保护组织的高级终端防护和威胁防护解决方案，可主动防御、检测并修复善于躲避的恶意软件攻击。
  - 远程访问VPN产品为用户可在差旅或远程工作期间提供安全无缝的企业网络和资源的远程访问。

终端安全产品系列

高级威胁防护

将零日保护扩展到终端和 web 浏览器。端点由威胁仿真、威胁提取及反勒索软件提供保护。

终端防护

Check Point 终端安全解决方案包括终端防护所需的一切：数据安全、网络安全、高级威胁防护、取证功能和远程访问 VPN，可提供全面的终端防护。

远程访问

通过多因素认证，合规扫描和加密功能，Check Point 远程访问 VPN 可为用户提供安全无缝的企业网络和资源访问。

资料来源：Check Point官网

安全管理产品

- 公司产品可整合多个安全层的管理，从而提高策略效率，并可通过单一控制台管理安全性。
  - R80.40网络安全管理工具具有跨所有网络和云环境的集中化管理控制功能，提高了操作效率，并降低了安全管理的复杂性。
  - SmartEvent事件管理通过单一视图对安全风险进行查看，以提供全面的威胁可见性。
  - Smart-1安全管理设备提供整合式的安全管理，从而实现跨网络、云端与移动设备的全面威胁可视性及控制。
  - 动态安全合规解决方案可对用户安全基础设施、网关、刀片、策略及配置设置进行持续实时监测。

安全管理产品系列

R80.40

网络安全：网关和管理

提供最具创新、最富成效的安全防护，使客户免受第五代网络攻击的威胁

事件管理

SmartEvent 威胁管理可完全集成，具有在单一位置进行日志记录、监控、事件关联和报告的功能。

安全管理设备

我们的 Smart-1 设备结合策略管理、监测及事件管理，针对一站式安全管理进行了优化。

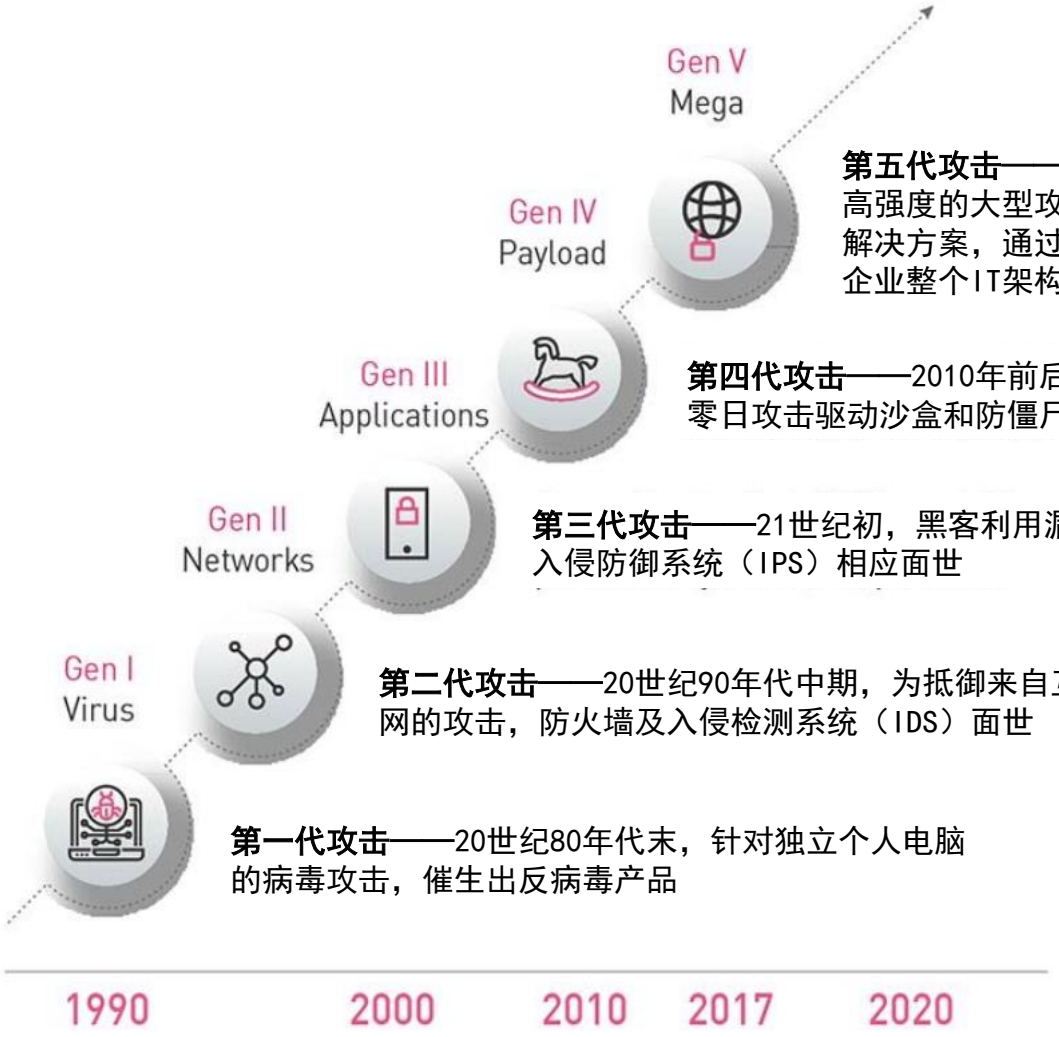
安全合规

利用所有 Check Point 产品的潜力来提高您的安全得分，避免人为错误的发生并保持监管合规性。

资料来源：Check Point官网

技术理念：针对多维度攻击的第五代网络安全

安全产品随着潜在威胁的升级而不断演进



第五代攻击——2017年前后，为应对多维度、高强度的大型攻击，需要更高级的威胁防御解决方案，通过**整合性的统一安全系统**保护企业整个IT架构

第四代攻击——2010年前后，定向、隐秘、多形态的零日攻击驱动沙盒和防僵尸产品的诞生

第三代攻击——21世纪初，黑客利用漏洞攻击应用程序，入侵防御系统（IPS）相应面世

第二代攻击——20世纪90年代中期，为抵御来自互联网的攻击，防火墙及入侵检测系统（IDS）面世

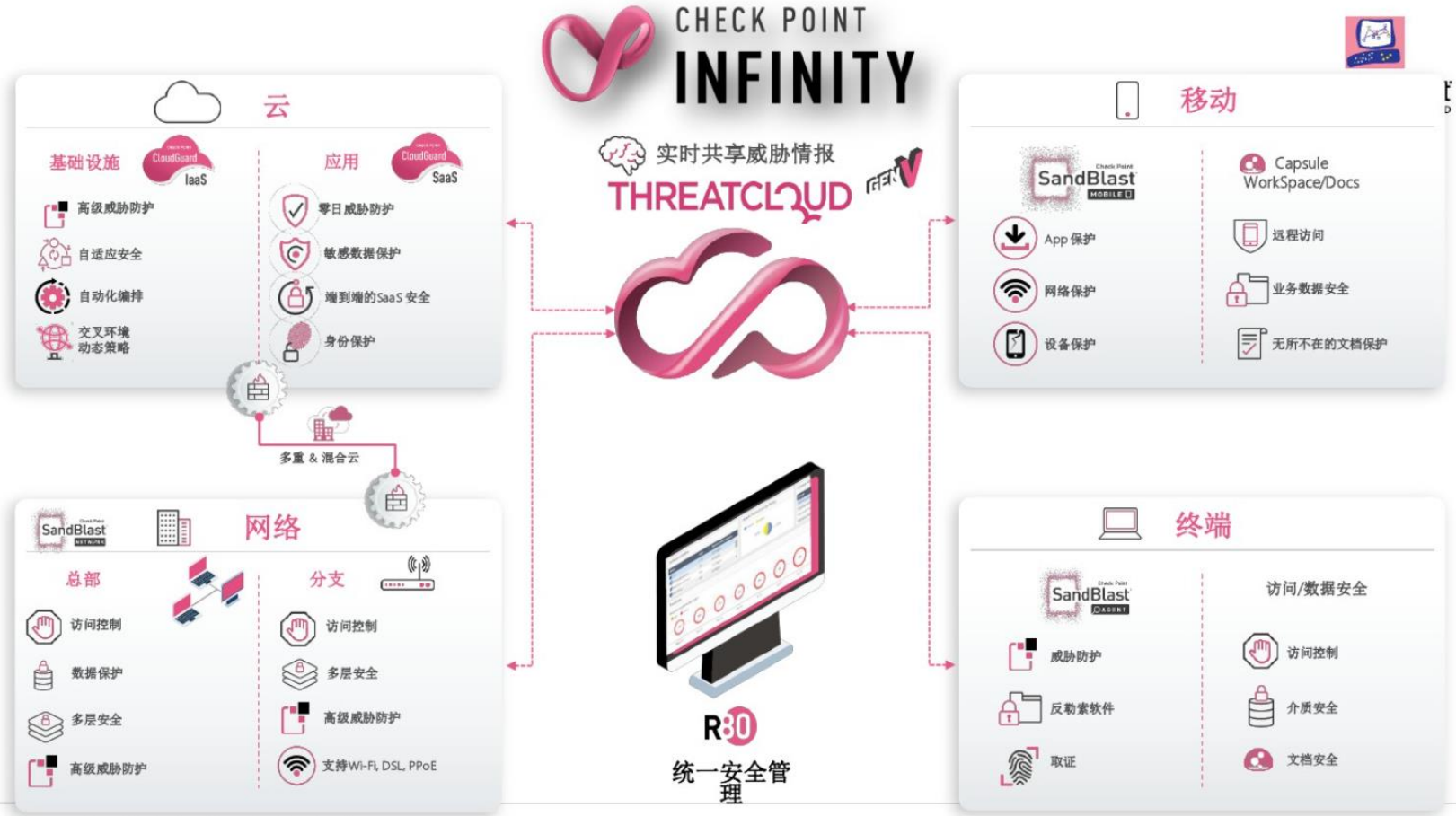
第一代攻击——20世纪80年代末，针对独立个人电脑的病毒攻击，催生出反病毒产品

资料来源：Check Point官网

Check Point Infinity：整合性第五代安全架构

- 公司在各产品线基础上推出Check Point Infinity整体解决方案——首个跨网络、云端和移动环境的整合性安全架构，可针对已知和未知目标性攻击提供高级别的威胁防护。

Check Point Infinity安全架构

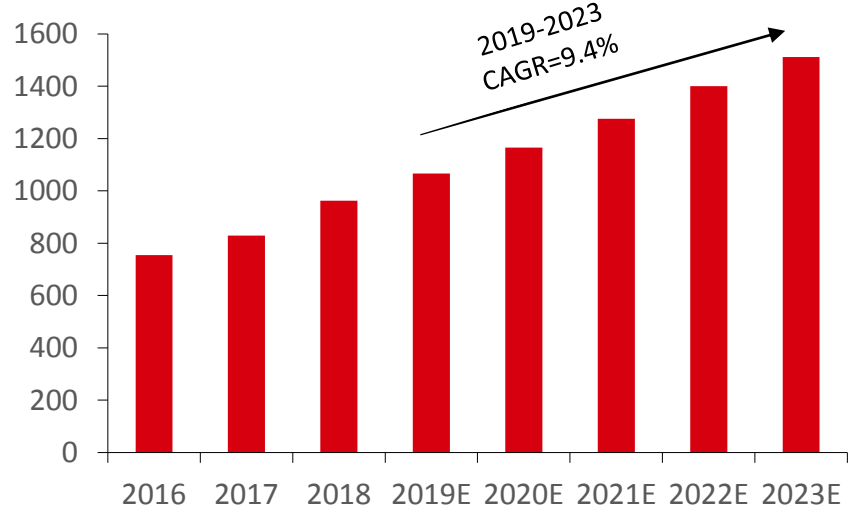


资料来源：Check Point官网

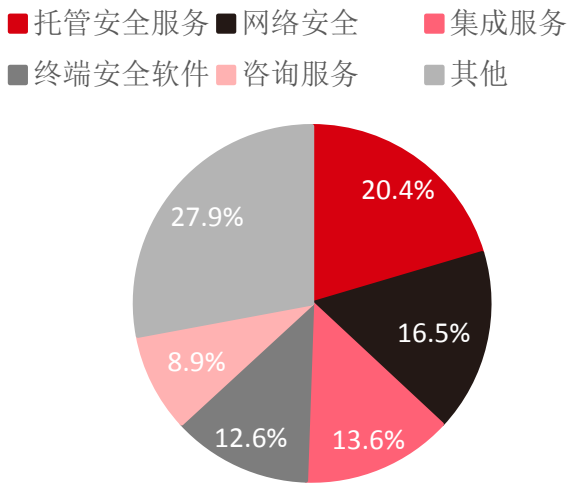
行业趋势：市场规模稳步增长

- 从市场规模来看，根据IDC数据，2018年全球信息安全支出（包括安全硬件、软件与服务）为963亿美元。IDC预测2023年全球信息安全支出规模将达到1512亿美元，2019-2023年间CAGR达9.4%。
- 从市场结构来看，IDC预计2019年最大的技术类别为托管安全服务，全球将支出超过210亿美元用于安全运营中心的全天候监视和管理；第二大技术类别将是网络安全硬件，包括统一威胁管理、防火墙以及入侵检测和防御技术；第三和第四大类别将是集成服务和端点安全软件。2019-2023年支出增长最快的技术类别将是托管安全服务（CAGR 13.9%），安全分析、情报、响应和编排软件（CAGR 10.5%）和咨询服务（CAGR 9.3%）。

全球信息安全市场收入规模（亿美元）



IDC对2019年全球信息安全市场结构的预测

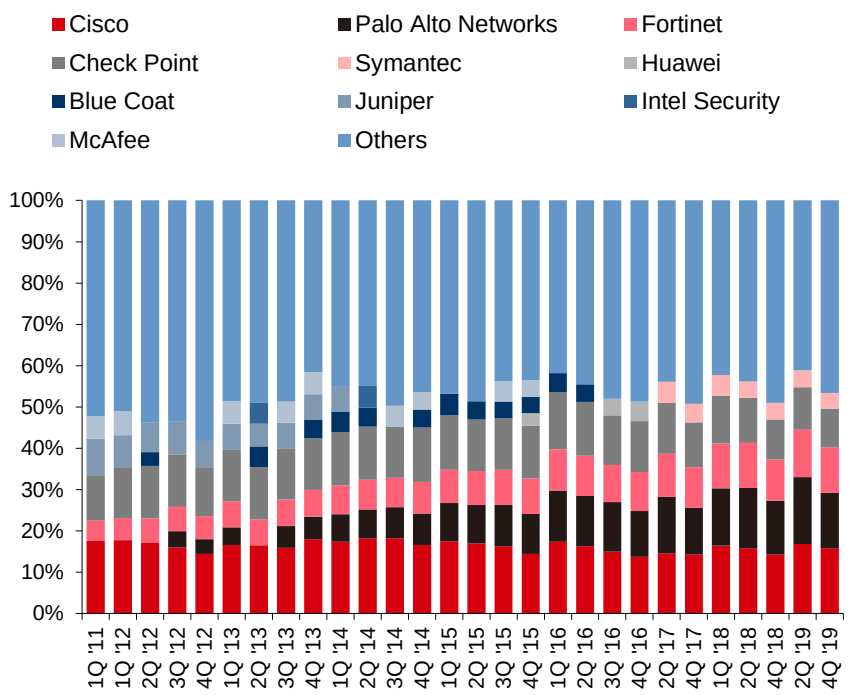


资料来源：IDC（含预测），中信证券研究部

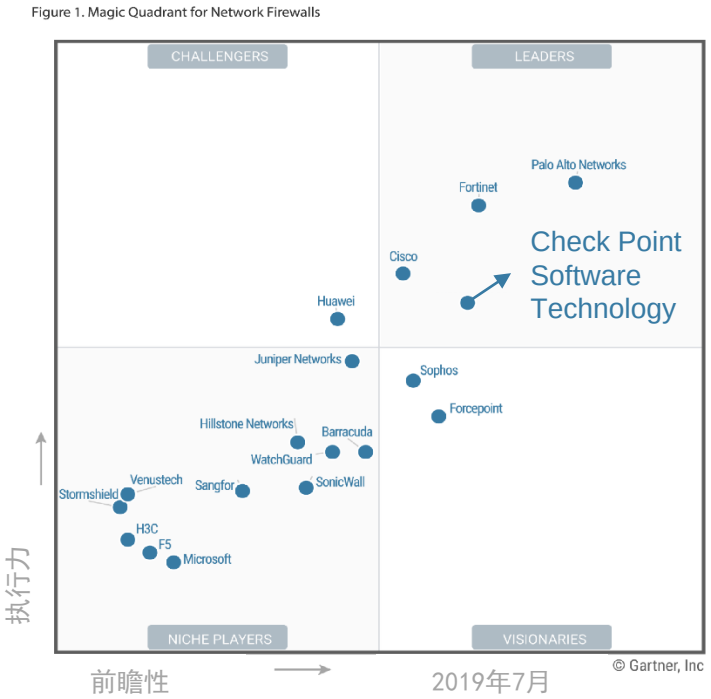
竞争格局：公司常年占据领导者地位

- 根据IDC数据，十年中Check Point在全球安全技术市场中份额稳居市场前列，尽管受Palo Alto Networks、Fortinet等竞争对手影响而略有下滑，但仍保持在10%左右。
- 截至2019年，公司在Gartner网络防火墙魔力象限中已有20次被评为行业领导者。

安全技术市场份额



Gartner网络防火墙魔力象限



资料来源：IDC，Gartner，中信证券研究部

合作伙伴生态系统实现互利互惠

- 渠道合作伙伴
  - 对合作伙伴的销售给予直接奖励，加快销售周期、创造增长动力，并向合作伙伴提供专家支持和资源，实现与合作伙伴的互利互惠，以加强与客户的关系，更好地为客户服务。
- 技术合作伙伴
  - Check Point与技术合作伙伴建立联盟，使客户可以使用联合解决方案来创建紧密联系、紧密集成的安全生态系统。

公司部分技术合作伙伴

Featured Partners

aws partner network

Google Cloud Premier Partner

Microsoft Azure

okta

servicenow

silver peak

splunk>

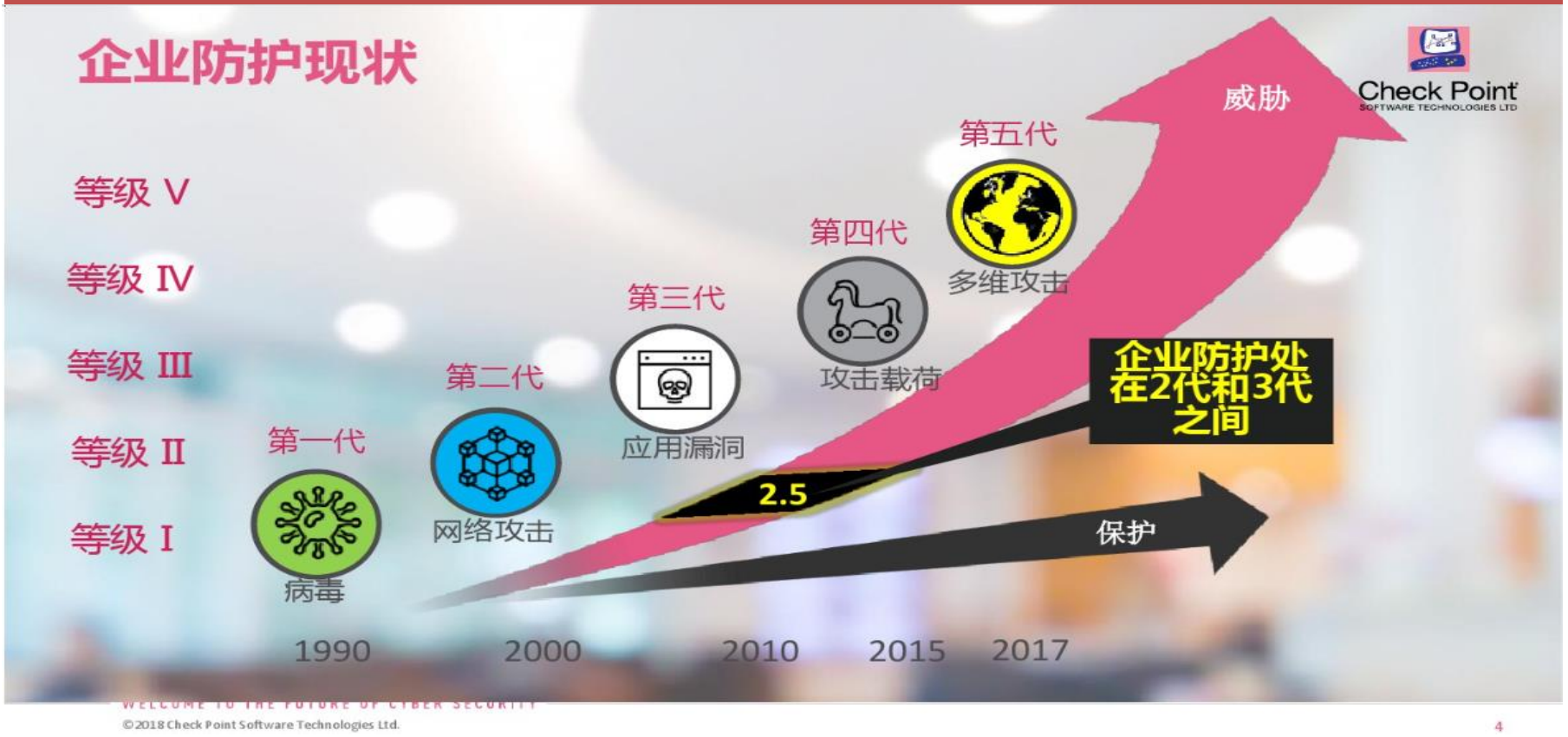
velocloud Now part of VMware

资料来源：Check Point官网

产品渗透率提升空间大

- Check Point 2018Q1的一项调查显示，多数企业停留在第二至第三代防护，仅有21%和3%的企业应用第四代和第五代防护，企业安全部署落后约10年。
- 公司对威胁的前瞻性有利于获取先发优势，有望通过提升产品渗透率进而推动业绩增长。

企业安全部署严重落后

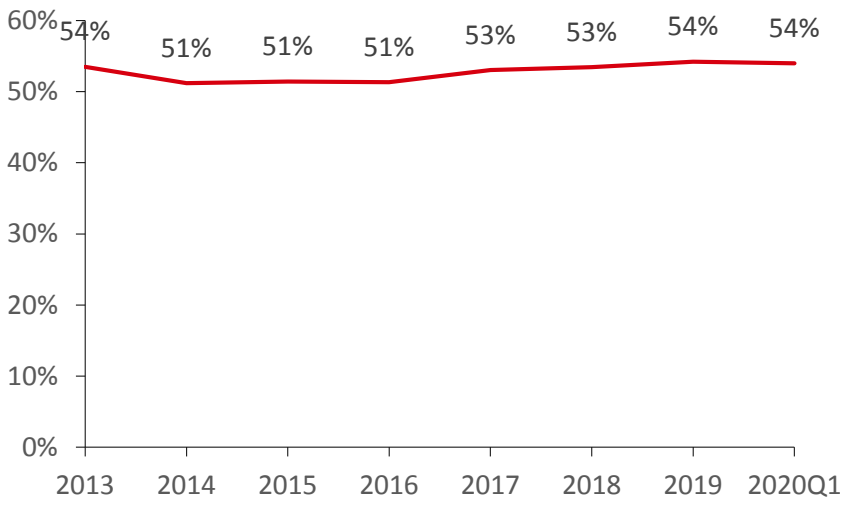


资料来源：Check Point官网

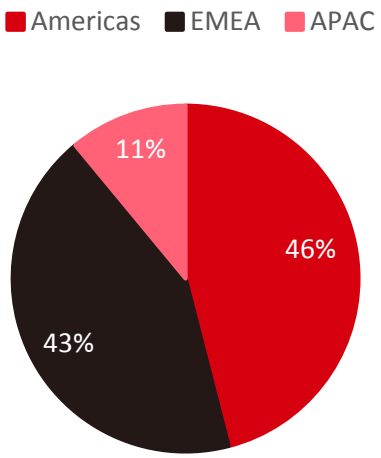
亚太地区市场尚待挖掘

- 从各地区营业收入来看，美洲及EMEA （欧洲、中东和非洲地区）为公司营收主要来源，APAC（亚太地区）收入有较大提升空间。
- 2020Q1公司在美洲、EMEA和APAC地区收入占比分别为46%、43%、11%。

公司海外营业收入占比



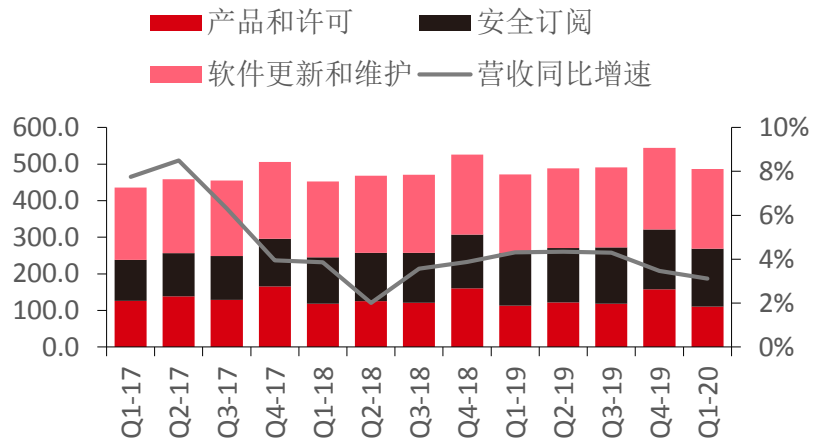
2020Q1营业收入结构（按地区）



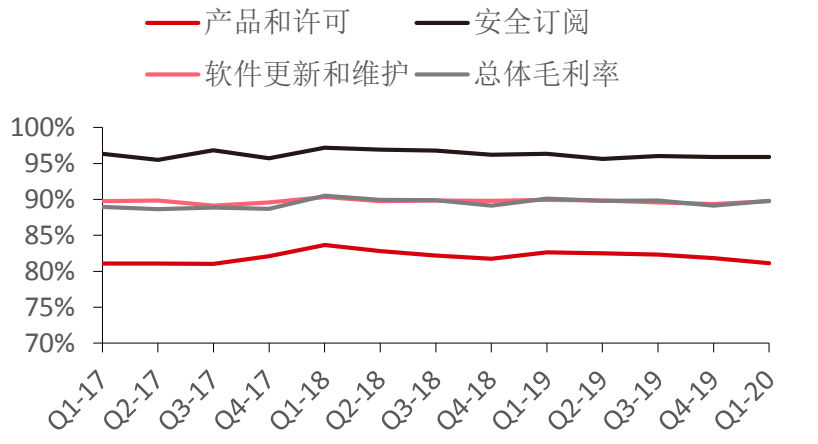
资料来源：公司财报，中信证券研究部

财务概要

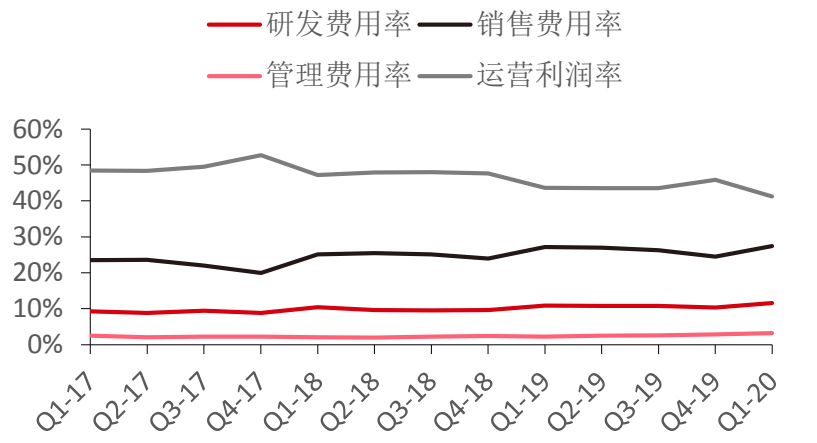
营业收入及同比增速（百万美元）



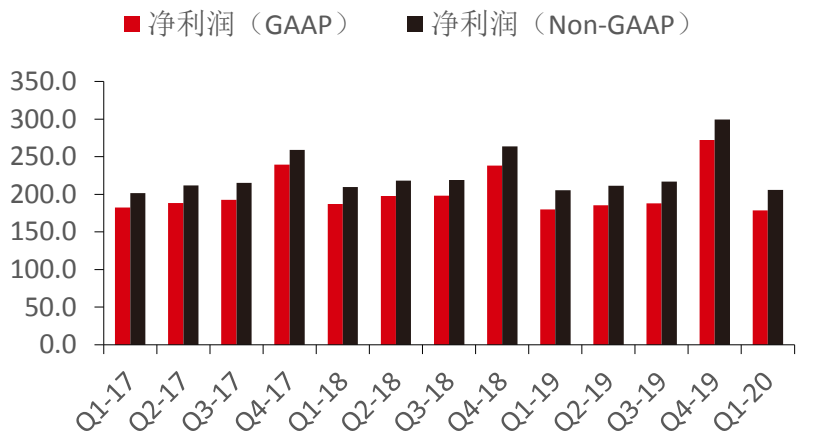
毛利率



费用率



净利润（百万美元）



资料来源：公司财报，中信证券研究部

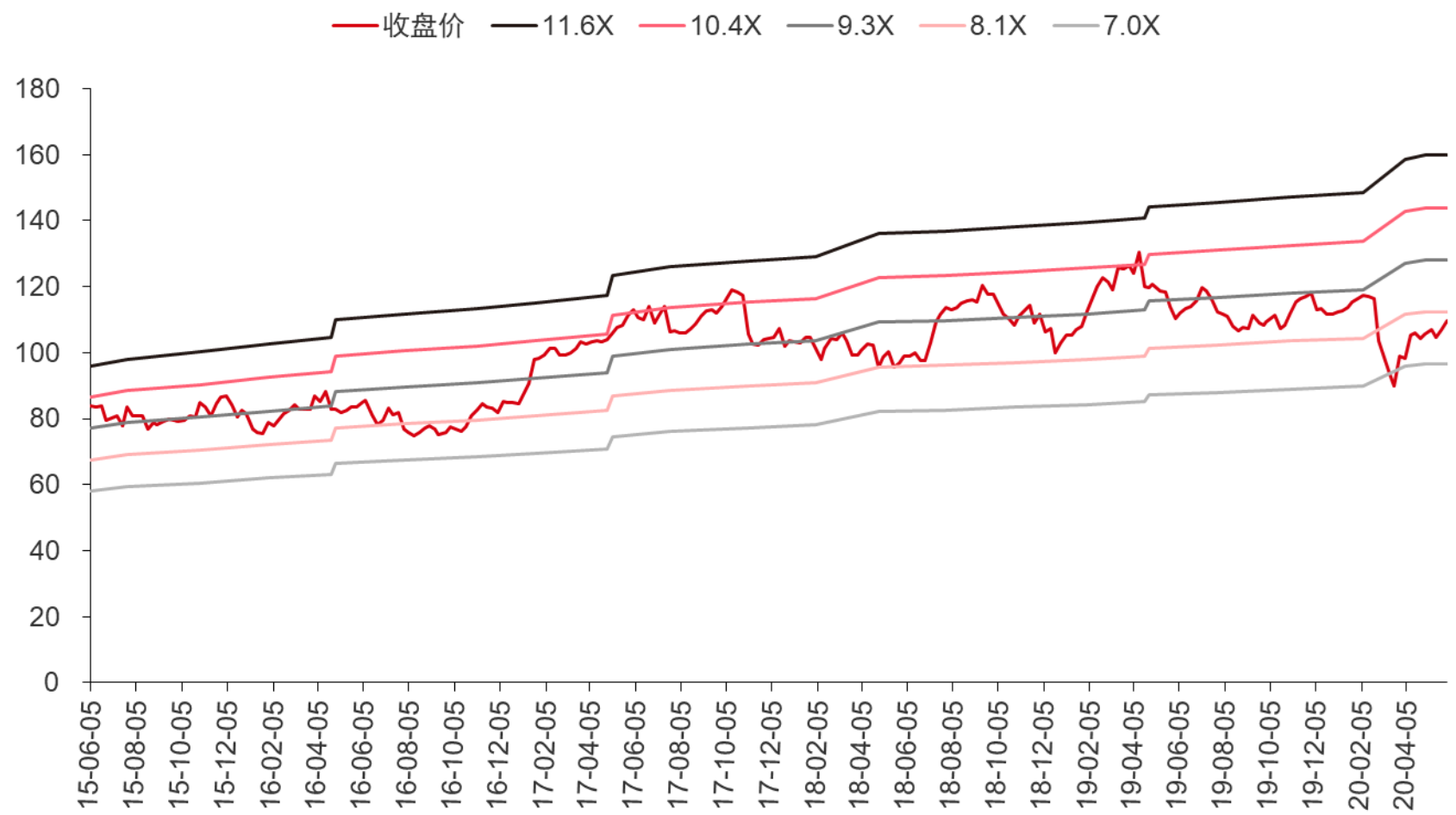
盈利预测

Check Point盈利预测					
年度	2018	2019	2020E	2021E	2022E
营业收入（百万美元）	1,916.48	1,994.8	2,011.5	2,073.1	2,103.6
YoY（%）	3%	4%	1%	3%	1%
净利润（GAAP，百万美元）	821.3	825.7	802.9	807.5	814.6
YoY（%）	2%	1%	-3%	1%	1%
净利润（Non-GAAP，百万美元）	911.1	933.0	908.4	917.2	923.6
YoY（%）	3%	2%	-3%	1%	1%
P/E（GAAP）	21	20	19	18	15
P/E（Non-GAAP）	19	18	17	16	15

资料来源：Thomson一致预期，中信证券研究部

估值水平

Check Point PS band



资料来源：Wind，中信证券研究部

中信证券
CITIC SECURITIES

感谢您的信任与支持！

THANKYOU

许英博（首席科技产业分析师）

执业证书编号：S1010510120041

陈俊云（前瞻研究高级分析师）

执业证书编号： S1010517080001

免责声明

分析师声明

主要负责撰写本研究报告全部或部分内容的分析师在此声明：（i）本研究报告所表述的任何观点均精准地反映了上述每位分析师个人对标的证券和发行人的看法；（ii）该分析师所得报酬的任何组成部分无论是在过去、现在及将来均不会直接或间接地与研究报告所表述的具体建议或观点相联系。

评级说明

投资建议的评级标准		评级	说明
报告中投资建议所涉及的评级分为股票评级和行业评级（另有说明的除外）。评级标准为报告发布日后6到12个月内的相对市场表现，也即：以报告发布日后的6到12个月内的公司股价（或行业指数）相对同期相关证券市场代表性指数的涨跌幅作为基准。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；美国市场以纳斯达克综合指数或标普500指数为基准；韩国市场以科斯达克指数或韩国综合股价指数为基准。	股票评级	买入	相对同期相关证券市场代表性指数涨幅20%以上
		增持	相对同期相关证券市场代表性指数涨幅介于5%～20%之间
		持有	相对同期相关证券市场代表性指数涨幅介于-10%～5%之间
		卖出	相对同期相关证券市场代表性指数跌幅10%以上
	行业评级	强于大市	相对同期相关证券市场代表性指数涨幅10%以上
		中性	相对同期相关证券市场代表性指数涨幅介于-10%～10%之间
		弱于大市	相对同期相关证券市场代表性指数跌幅10%以上

其他声明

本研究报告由中信证券股份有限公司或其附属机构制作。中信证券股份有限公司及其全球的附属机构、分支机构及联营机构（仅就本研究报告免责条款而言，不含CLSA group of companies），统称为“中信证券”。

法律主体声明

本研究报告在中华人民共和国（香港、澳门、台湾除外）由中信证券股份有限公司（受中国证券监督管理委员会监管，经营证券业务许可证编号：Z20374000）分发。本研究报告由下列机构代表中信证券在相应地区分发：在中国香港由CLSA Limited分发；在中国台湾由CL Securities Taiwan Co., Ltd.分发；在澳大利亚由CLSA Australia Pty Ltd.（金融服务牌照编号：350159）分发；在美国由CLSA group of companies（CLSA Americas, LLC（下称“CLSA Americas”）除外）分发；在新加坡由CLSA Singapore Pte Ltd.（公司注册编号：198703750W）分发；在欧盟与英国由CLSA Europe BV或 CLSA （UK）分发；在印度由CLSA India Private Limited分发（地址：孟买（400021）Nariman Point的Dalamal House 8层；电话号码：+91-22-66505050；传真号码：+91-22-22840271；公司识别号：U67120MH1994PLC083118；印度证券交易委员会注册编号：作为证券经纪商的INZ000001735，作为商人银行的INM000010619，作为研究分析商的INH000001113）；在印度尼西亚由PT CLSA Sekuritas Indonesia分发；在日本由CLSA Securities Japan Co., Ltd.分发；在韩国由CLSA Securities Korea Ltd.分发；在马来西亚由CLSA Securities Malaysia Sdn Bhd分发；在菲律宾由CLSA Philippines Inc.（菲律宾证券交易所及证券投资者保护基金会员）分发；在泰国由CLSA Securities (Thailand) Limited分发。

针对不同司法管辖区的声明

中国：根据中国证券监督管理委员会核发的经营证券业务许可，中信证券股份有限公司的经营范围包括证券投资咨询业务。

美国：本研究报告由中信证券制作。本研究报告在美国由CLSA group of companies（CLSA Americas除外）仅向符合美国《1934年证券交易法》下15a-6规则定义且CLSA Americas提供服务的“主要美国机构投资者”分发。对身在美国的任何人士发送本研究报告将不被视为对本报告中所评论的证券进行交易的建议或对本报告中所载任何观点的背书。任何从中信证券与CLSA group of companies获得本研究报告的接收者如果希望在美国交易本报告中提及的任何证券应当联系CLSA Americas。

新加坡：本研究报告在新加坡由CLSA Singapore Pte Ltd.（资本市场经营许可持有人及受豁免的财务顾问），仅向新加坡《证券及期货法》s.4A（1）定义下的“机构投资者、认可投资者及专业投资者”分发。根据新加坡《财务顾问法》下《财务顾问（修正）规例（2005）》中关于机构投资者、认可投资者、专业投资者及海外投资者的第33、34及35 条的规定，《财务顾问法》第25、27及36条不适用于CLSA Singapore Pte Ltd.。如对本报告存有疑问，还请联系CLSA Singapore Pte Ltd.（电话：+65 6416 7888）。MCI (P) 086/12/2019。

加拿大：本研究报告由中信证券制作。对身在加拿大的任何人士发送本研究报告将不被视为对本报告中所评论的证券进行交易的建议或对本报告中所载任何观点的背书。

欧盟与英国：本研究报告在欧盟与英国归属于营销文件，其不是按照旨在提升研究报告独立性的法律要件而撰写，亦不受任何禁止在投资研究报告发布前进行交易的限制。本研究报告在欧盟与英国由CLSA （UK）或CLSA Europe BV发布。CLSA （UK）由（英国）金融行为管理局授权并接受其管理，CLSA Europe BV 由荷兰金融市场管理局授权并接受其管理，本研究报告针对由相应本地监管规定所界定的在投资方面具有专业经验的人士，且涉及到的任何投资活动仅针对此类人士。若您不具备投资的专业经验，请勿依赖本研究报告。对于由英国分析员编纂的研究资料，其由CLSA （UK）与CLSA Europe BV制作并发布。就英国的金融行业准则与欧洲其他辖区的《金融工具市场指令II》，本研究报告被制作并意图作为实质性研究资料。

澳大利亚：本研究报告在澳大利亚由CLSA Australia Pty Ltd.（金融服务牌照编号：350159）仅向《公司法（2001）》第761G条定义下的批发客户分发，并非意图分发给任何零售客户。

一般性声明

本研究报告对于收件人而言属高度机密，只有收件人才能使用。本研究报告并非意图发送、发布给在当地法律或监管规则下不允许向其发送、发布该研究报告的人员。本研究报告仅为参考之用，在任何地区均不应被视为买卖任何证券、金融工具的要约或要约邀请。中信证券并不因收件人收到本报告而视其为中信证券的客户。本报告所包含的观点及建议并未考虑个别客户的特殊状况、目标或需要，不应被视为对特定客户关于特定证券或金融工具的建议或策略。对于本报告中提及的任何证券或金融工具，本报告的收件人须保持自身的独立判断。

本报告所载资料的来源被认为是可靠的，但中信证券不保证其准确性或完整性。中信证券并不对使用本报告所包含的材料产生的任何直接或间接损失或与此有关的其他损失承担任何责任。本报告提及的任何证券或金融工具均可能含有重大的风险，可能不易变卖以及不适合所有投资者。本报告所提及的证券或金融工具的价格、价值及收益可能会受汇率影响而波动。过往的业绩并不能代表未来的表现。

本报告所载的资料、观点及预测均反映了中信证券在最初发布该报告日期当日分析师的判断，可以在不发出通知的情况下做出更改，亦可因使用不同假设和标准、采用不同观点和分析方法而与中信证券其它业务部门、单位或附属机构在制作类似的其他材料时所给出的意见不同或者相反。中信证券并不承担提示本报告的收件人注意该等材料的责任。中信证券通过信息隔离墙控制中信证券内部一个或多个领域的信息向中信证券其他领域、单位、集团及其他附属机构的流动。负责撰写本报告的分析师的薪酬由研究部门管理层和中信证券高级管理层全权决定。分析师的薪酬不是基于中信证券投资银行收入而定，但是，分析师的薪酬可能与投行整体收入有关，其中包括投资银行、销售与交易业务。

若中信证券以外的金融机构发送本报告，则由该金融机构为此发送行为承担全部责任。该机构的客户应联系该机构以交易本报告中提及的证券或要求获悉更详细信息。本报告不构成中信证券向发送本报告金融机构之客户提供的投资建议，中信证券以及中信证券的各个高级职员、董事和员工亦不为（前述金融机构之客户）因使用本报告或报告载明的内容产生的直接或间接损失承担任何责任。