

科技先锋系列报告91

Palo Alto Networks (PANW.N) : 云安全践行者



许英博 首席科技产业分析师

陈俊云 前瞻研究高级分析师

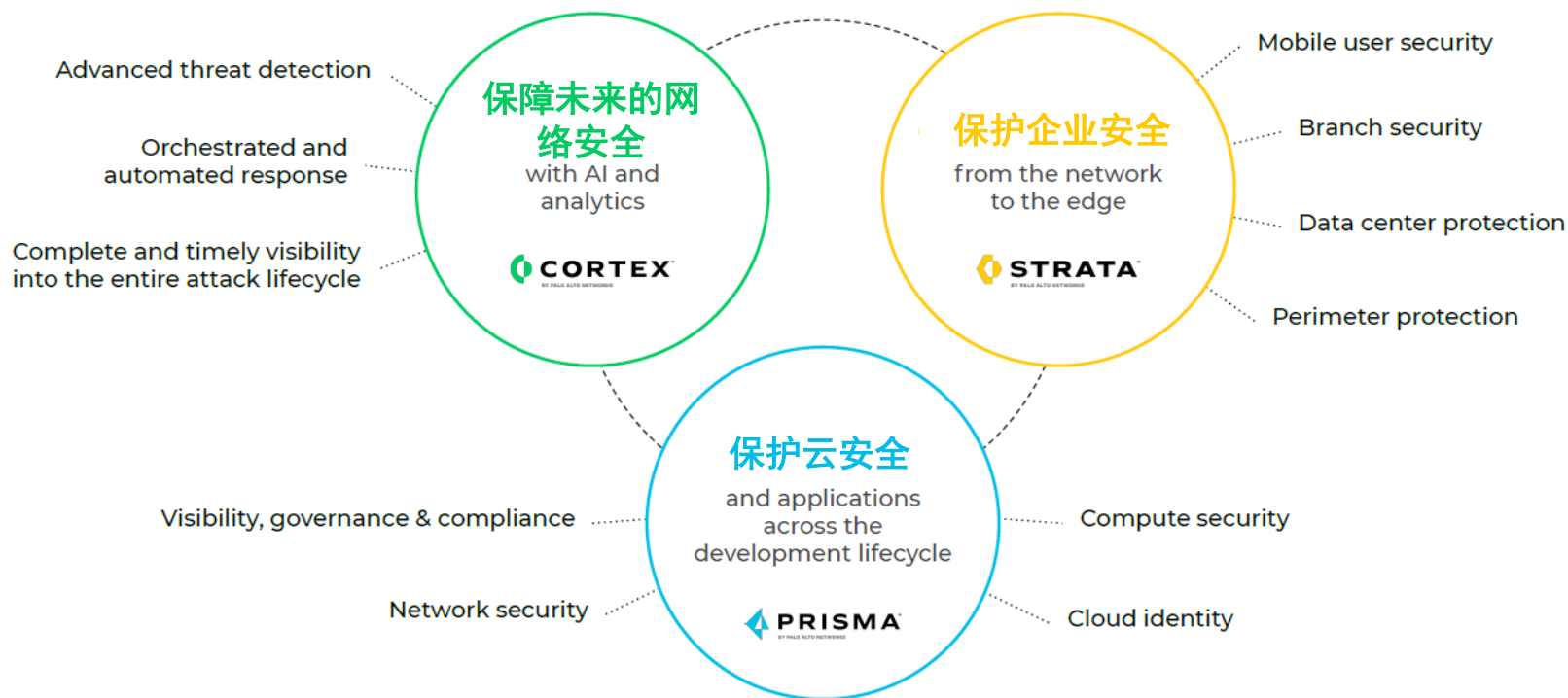
中信证券研究部·前瞻研究

2020年5月28日

Palo Alto Networks: 全球网络安全领导者

- Palo Alto Networks成立于2005年，是全球网络安全行业的领军者。公司借助人工智能、分析、自动化和业务流程编排的最新突破，通过提供集成式的平台，携手不断成长的合作伙伴生态系统，为数以万计企业的云、网络和移动设备提供前沿的安全保护。公司的愿景是打造更安全无忧的世界。
- 截至FY2020Q3，公司客户数已达73,000家，覆盖全球150多个国家和地区。

Palo Alto Networks全面安全解决方案



- 公司提供行业领先的网络安全套件防御攻击，帮助组织实现网络转型，同时对各个位置的用户、应用和数据提供一致保护。

企业安全系列产品

类别	产品	介绍
新一代防火墙	PA-series 物理防火墙系列	通过易于部署和操作的防御优先型架构，可以有效地简化并增强安全防护，为整个网络边界（从总部和办公区、分支机构和数据中心到您的移动和远程员工）提供一致的保护。
	VM-series 虚拟防火墙系列	通过分段和威胁防御，帮助保护私有云和公有云部署的安全。
订阅产品	Threat Prevention 威胁防御	一次扫描即可阻止已知的客户端和服务端漏洞利用、恶意软件以及命令和控制攻击，而不会妨碍网络流量。基于有效载荷的签名能够自动更新（确保安全产品最新），可阻止高级威胁。Threat Prevention 采用 WildFire，能够提供零信任模型中的分层防御。
	URL Filtering URL过滤	让所有用户安全地访问 Web。PAN-DB 可自动防御利用 Web 作为攻击媒介发起的攻击，包括电子邮件中的网络钓鱼链接、网络钓鱼站点、基于 HTTP 的（命令和控制）攻击、恶意软件网站以及携带漏洞利用工具包的页面。通过一套管理和维护策略，保护您的组织免受各种安全、法律、法规、合规和可接受使用风险的侵害。然后，与 WildFire 共享威胁数据。
	WildFire	检测并防止未知攻击。WildFire® 恶意软件防御服务将动态和静态分析、创新机器学习技术与开创性裸机分析环境进行了结合，抵御高度规避的零日漏洞利用和恶意软件。WildFire 会根据检测结果，在攻击生命周期中自动创建新防护方法，同时不断更新使用的全部技术。
	DNS Security 服务	使用预测分析阻止利用 DNS 发动的命令和控制 (C2) 或数据窃取的攻击。通过与新一代防火墙紧密集成提供自动防护。
	SD-WAN	安全可靠的软件定义广域网，能够针对分支机构和零售店的云应用提供最佳用户体验，而不影响安全性。
	GlobalProtect	能够面向移动用户提供新一代防火墙的保护，保护用户免受恶意应用流量、网络钓鱼、凭证盗窃等侵害。
	Palo Alto Networks Enterprise DLP	能够发现、监视和保护组织的敏感数据（如 PII 和知识产权），最大程度地降低数据泄露风险，并增强数据隐私保护和合规性。
网络安全管理	Panorama	具有易于实施的集中管理功能，使用户能够了解网络流量和威胁，并能在任何地方管理防火墙。

- Prisma 能通过提供业界最全面的云安全功能，由内而外地保护云，助客户实现云转型并保护各个位置的用户、应用和数据。

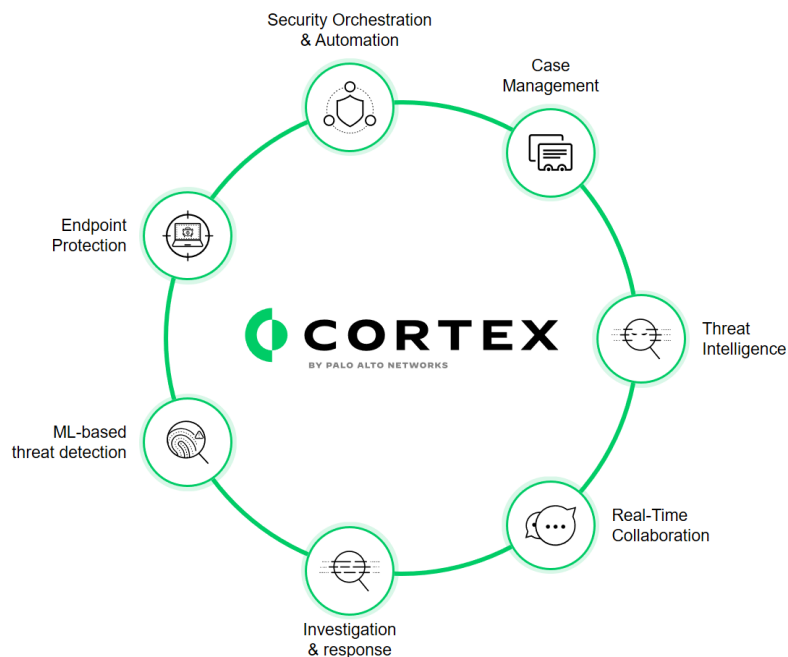
云安全系列产品

产品	介绍
Prisma Access	安全访问服务边缘 (SASE) 平台，能够将全球各地的移动用户、分支机构和零售店互联并为其提供保护。
Prisma SaaS	SaaS 应用安全产品，能够保护数据，监管数据并确保数据合规，帮助组织安全地采用 SaaS。
Prisma Cloud	云原生安全平台，能够在多云环境中提供一致、全面的可视性、威胁防御、合规保证和数据保护。
VM-Series 虚拟防火墙系列	利用敏捷的内联网络安全和威胁防御功能为公共云和私有云、虚拟化数据中心及分支机构提供一致的保护。

- 公司提供业界最全面的安全运营产品套件，让企业具备一流的检测、调查、自动化和响应能力。

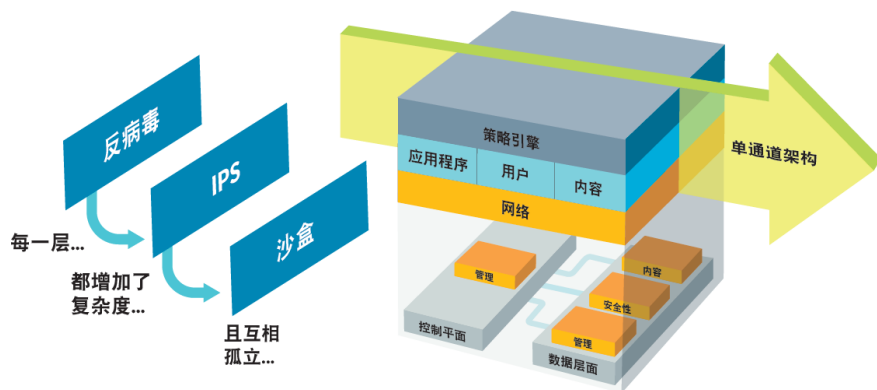
Cortex系列产品

产品	介绍
Cortex XDR	完全集成的端点、网络和云数据的检测和响应平台。
Cortex XSOAR	借助业界领先的安全编排、自动化和响应平台 Cortex XSOAR，可以管理警报，标准化流程并自动化 300 多种第三方产品的操作。
Cortex Data Lake	帮助客户收集、转换和集成企业的安全数据来高效使用 Palo Alto Networks 解决方案。
AutoFocus	能够提供高精度威胁情报，帮助企业提高防御、调查和响应能力。

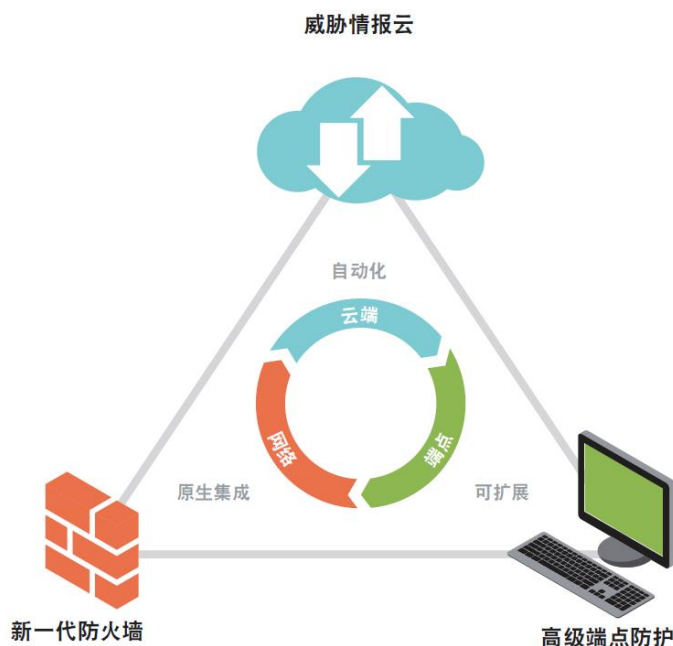


- Palo Alto Networks新一代防火墙为企业、服务提供商和政府提供以预防为主的网络安全方法。新一代防火墙以单通道方式检查所有端口上的全部流量，包括所有应用、威胁和内容，然后将流量与用户绑定，从而提供了有关应用、关联内容和用户身份的全面情境信息，以此为基础来做出安全策略决策。
- 与传统方法相比，新一代防火墙有利于打造原生集成的安全平台，降低成本和复杂性，而提高安全性与易用性，实现从网络到云端和端点的一致安全架构。

传统安全技术与新一代防火墙对比



从网络到云端和端点的一致安全架构



集成式平台：Security Operating Platform

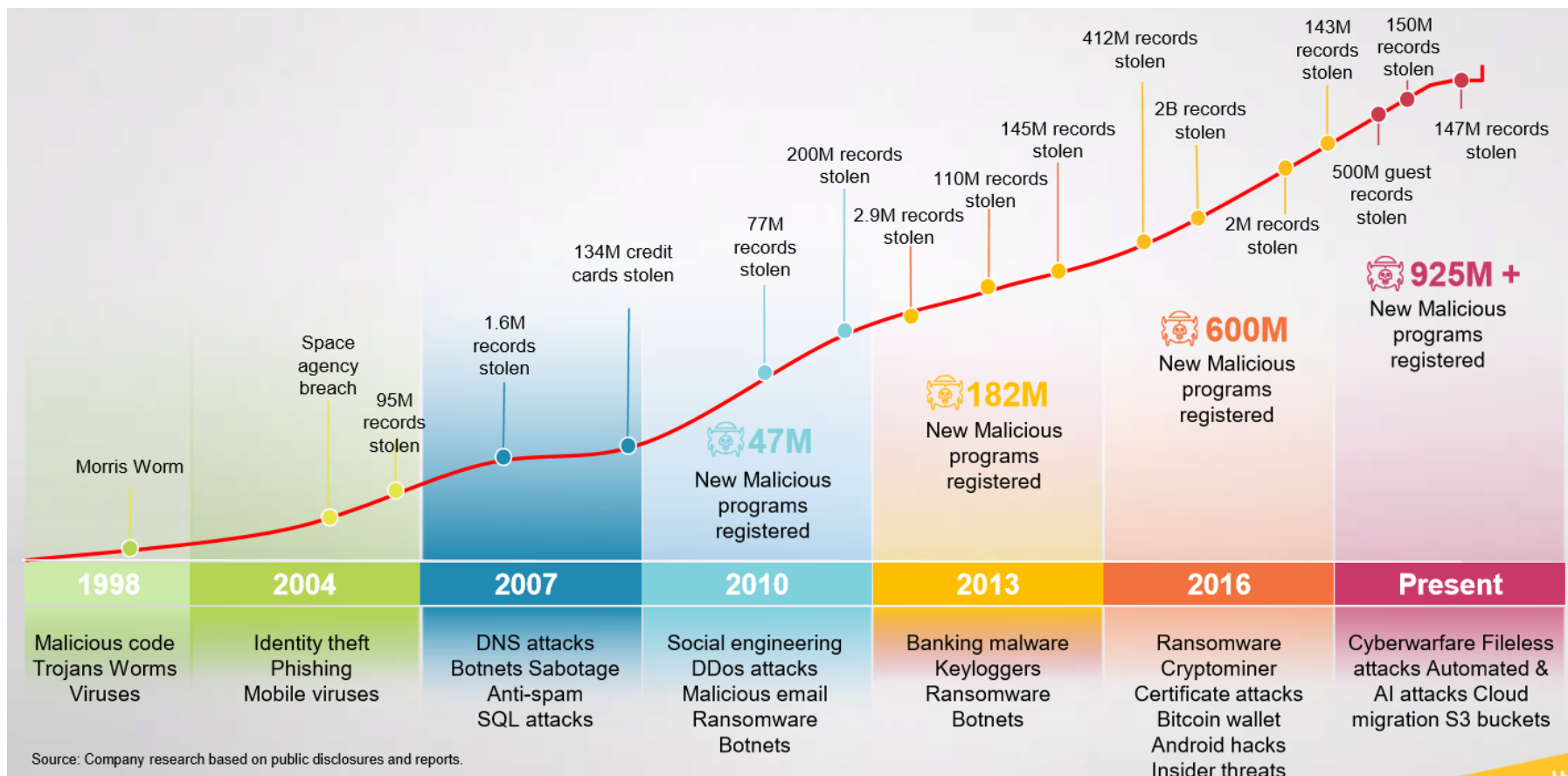
- Security Operating Platform通过分析功能实现例行任务及实施的自动化，以成功阻止网络攻击。通过整个平台以及与合作伙伴的紧密集成，简化安全措施，妥善保护用户、应用程序及数据的安全。

Palo Alto Networks安全平台



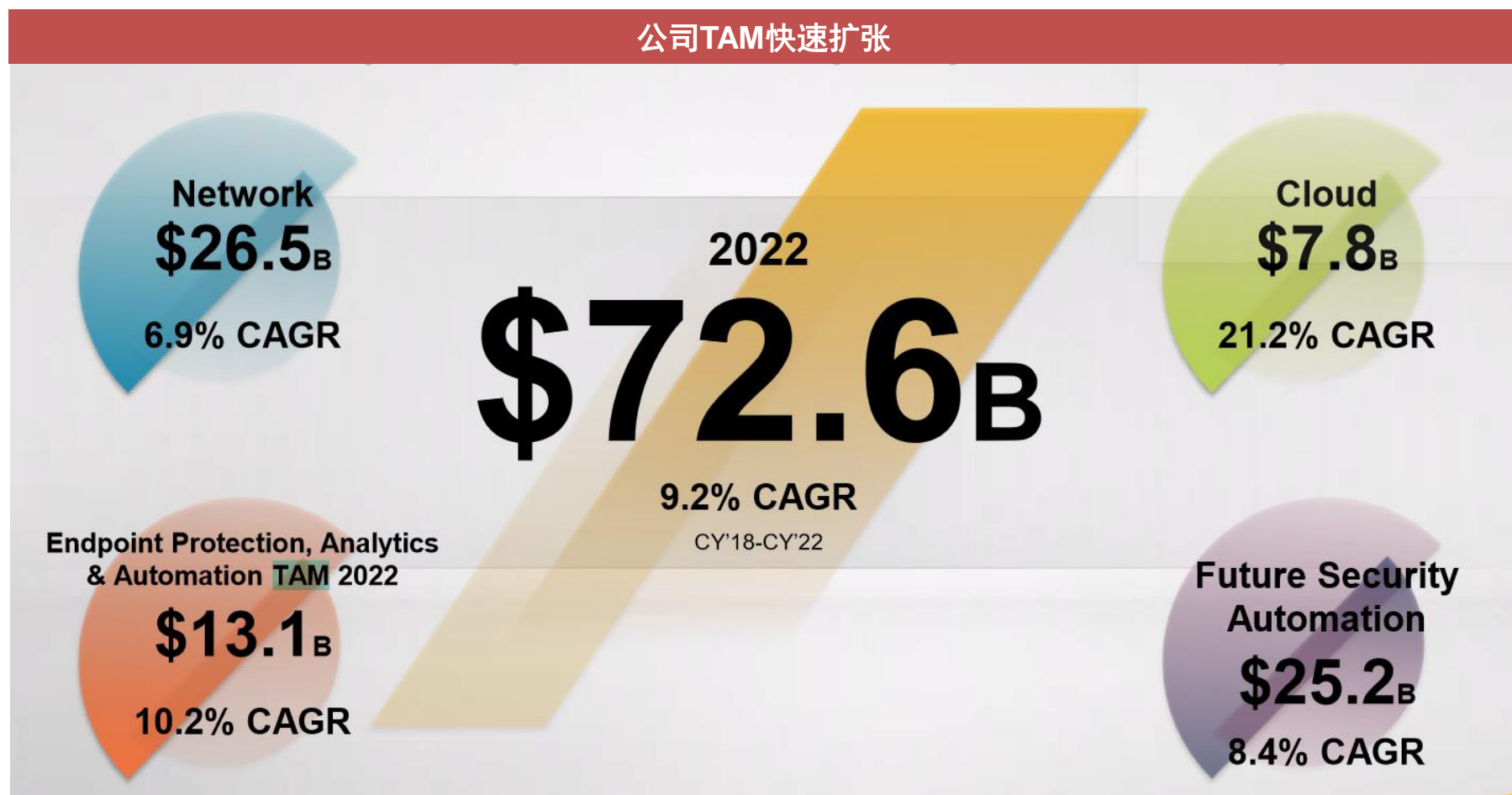
行业趋势：复杂IT系统架构推升安全需求

网络威胁形势日益严峻



行业趋势：网络安全需求不断升级，推升TAM

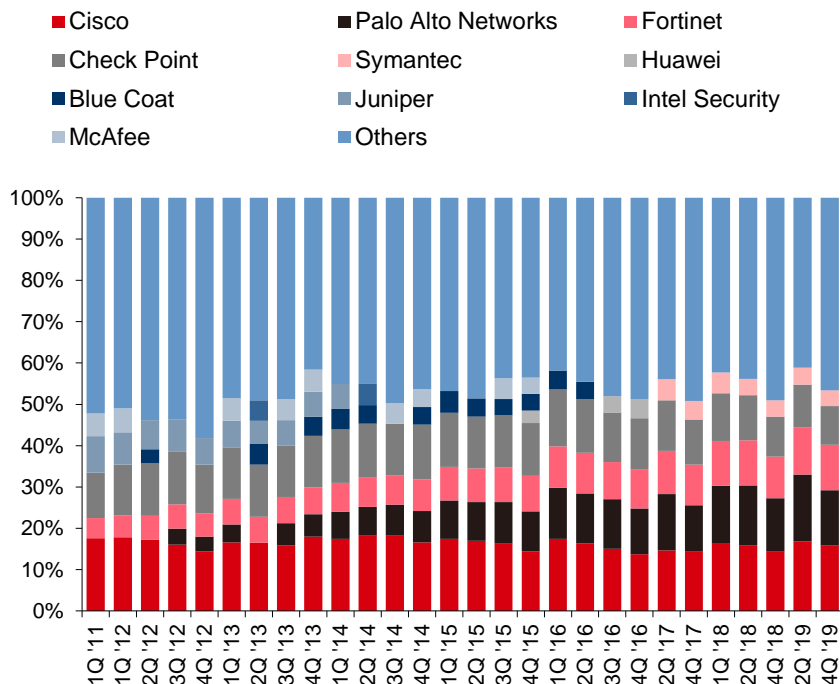
- 用户对网络安全需求的升级推升市场空间。据Gartner的预测和公司内部测算，2022年公司对应TAM可达726亿美元，2018-2022年CAGR约9.2%。公司各业务板块市场空间均有高速增长，其中云安全市场增速最快。



竞争格局：公司为防火墙市场领导者

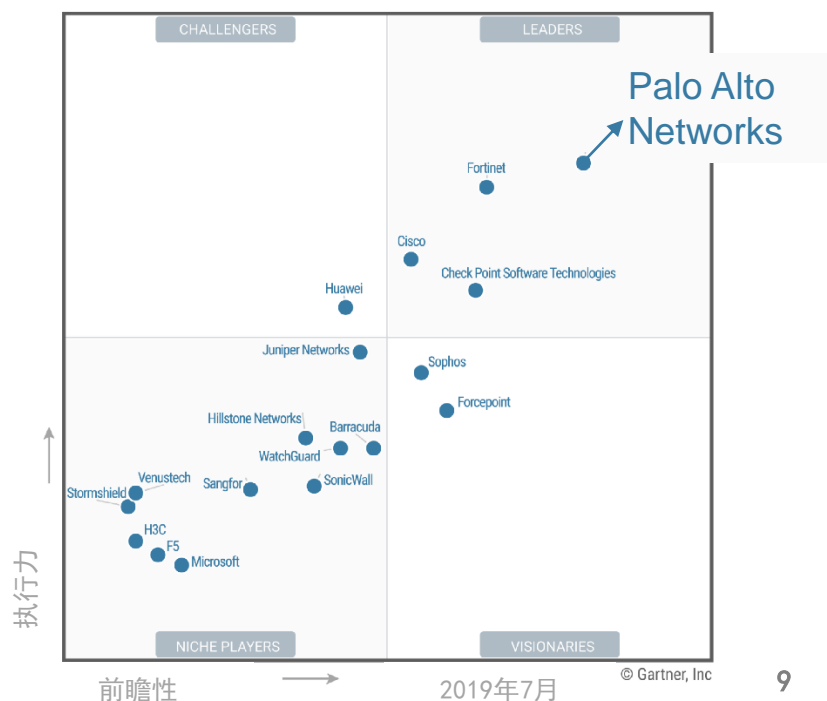
- 根据IDC数据，Palo Alto Networks在全球安全技术市场中份额保持增长态势，尽管近年来增速放缓并略有降低，但份额稳居市场前两名，2019Q4市场份额约占13.4%。
- 根据Gartner评估，公司在网络防火墙魔力象限中连续八年被评为领导者，前瞻性与执行力均为行业首位。

安全技术市场份额



Gartner网络防火墙魔力象限

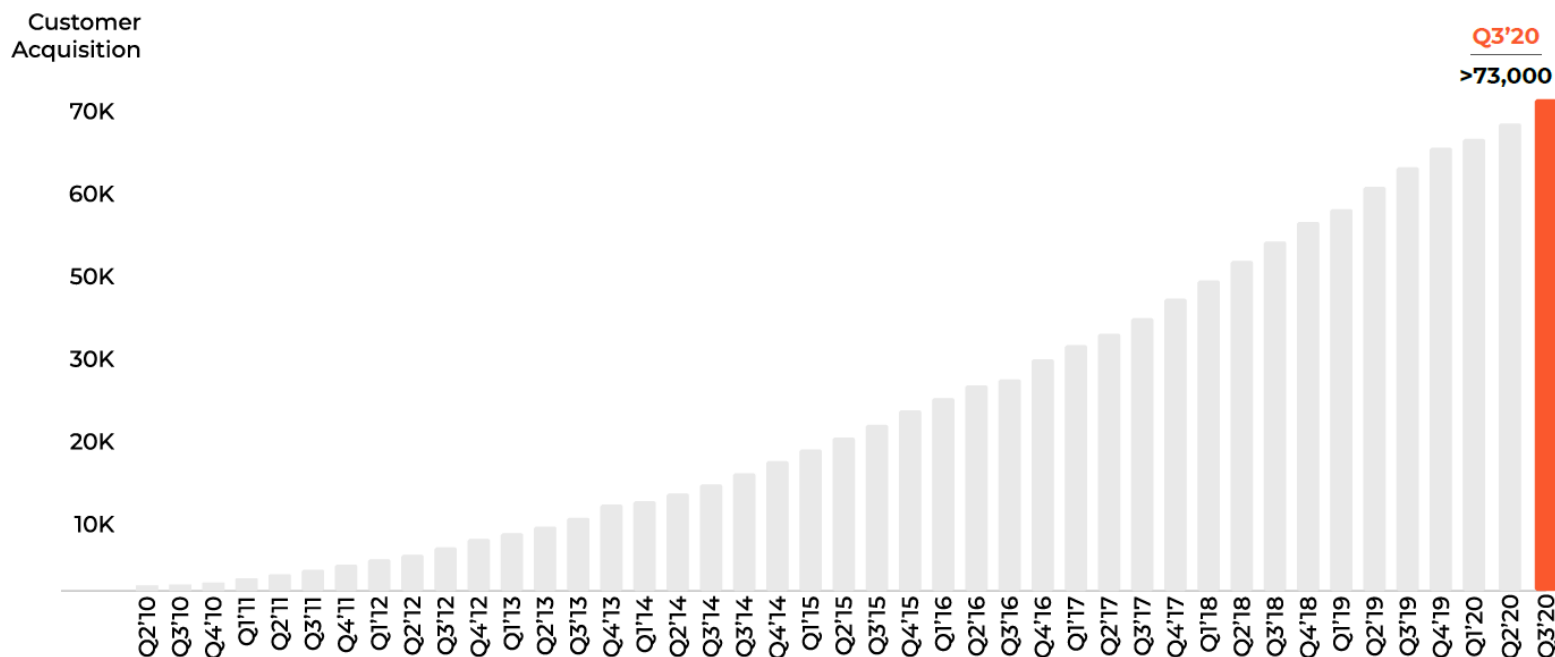
Figure 1. Magic Quadrant for Network Firewalls



成长性：用户数量持续增长

- 在网络安全威胁日益复杂的行业趋势下，公司凭借领先的技术优势成为全球企业安全解决方案的领导者，客户数量十年来持续增长。
- 截至FY2020Q3，公司客户已超过73,000家，较去年同期增加约11,000家，较上季度增加约3,000家，增长势头强劲。

Palo Alto Networks客户数量



Customers represent all customers acquired since inception. A customer is defined as accounts that have purchased products and services excluding not-for-resale services.

成长性：积极并购扩展产品线

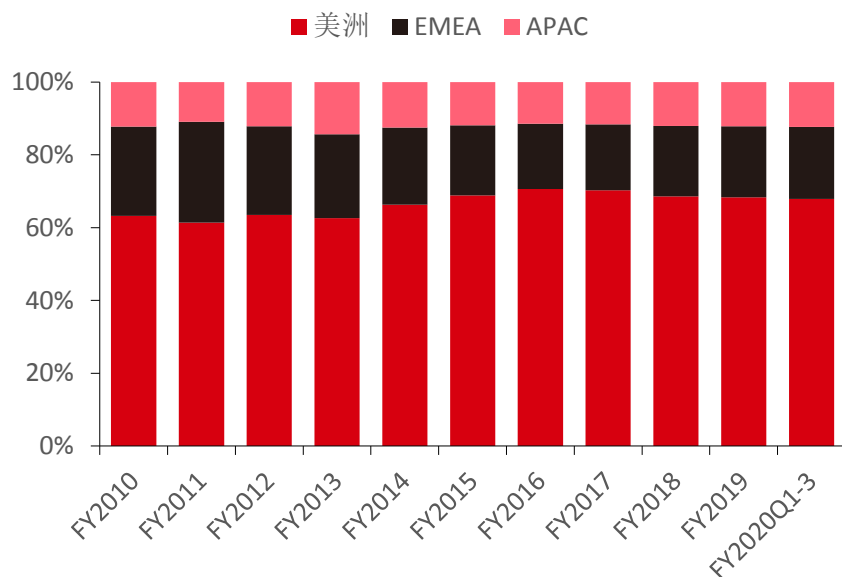
- 公司不断进行重要并购扩展产品线，为用户提供更全面的安全保护。

近五年公司并购活动			
时间	收购公司名称	介绍	收购金额 (百万美元)
2019.7.9	Twistlock Ltd.	容器安全公司	378.1
2019.6.12	PureSec Ltd.	为无服务器的架构提供网络安全解决方案	36.8
2019.3.28	Demisto, Inc.	从事安全编排、自动化和响应技术（SOAR）	474.2
2018.10.12	RedLock Inc.	云安全技术公司，该公司的云安全分析技术使得公司扩展了公有云安全服务能力	158.2
2018.3.26	Evident.io, Inc.	云安全技术公司，该公司的云服务基础架构保护技术使得公司扩展了基于API的公有云安全服务能力	292.9
2018.4.24	Cyber Secdo Ltd.	从事终端检测和响应（EDR）技术的公司	82.7
2017.2.27	LightCyber Ltd.	网络安全技术公司，该收购扩展了行为分析技术	103.1

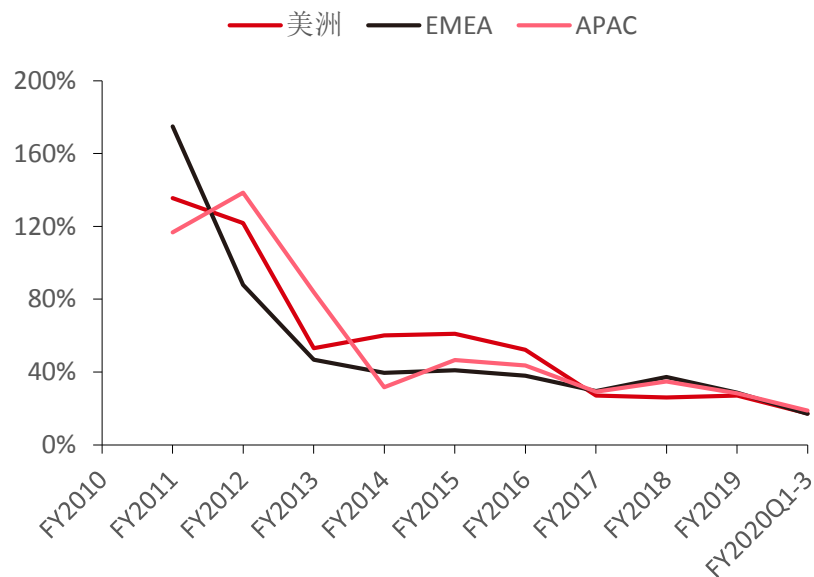
成长性：海外市场潜力巨大

- 从各地区营业收入来看，近年各地区营业收入占比较为稳定，海外地区收入占比维持在30%左右，有较大提升空间。
- FY2020Q1-3美洲地区收入占比68%，同比+17%；EMEA（欧洲、中东和非洲地区）占比20%，同比+17%；APAC（亚太地区）占比12%，同比+19%。

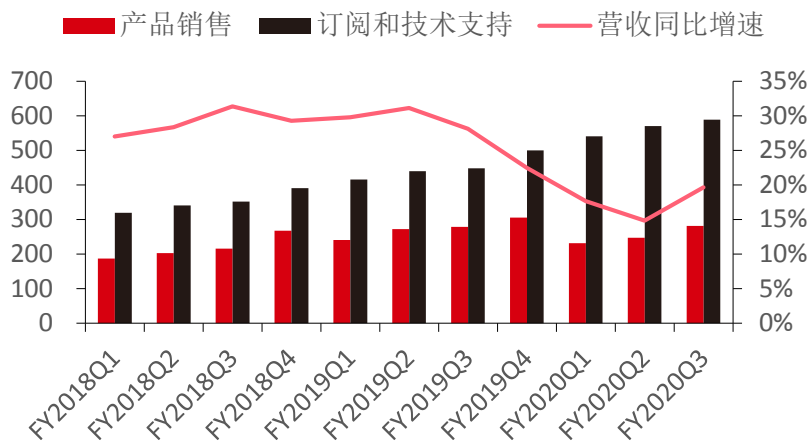
公司各地区营业收入占比



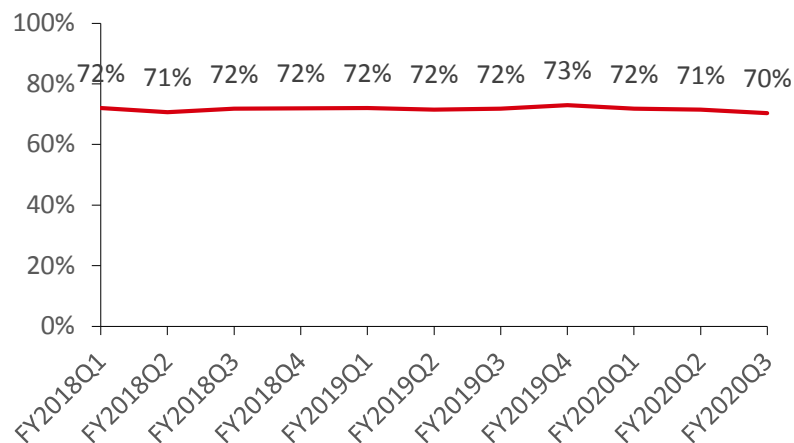
各地区营业收入同比增速



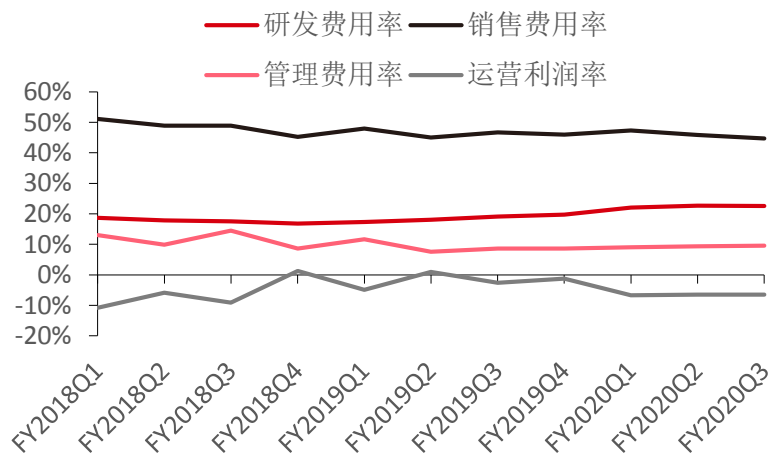
营业收入及同比增速（百万美元）



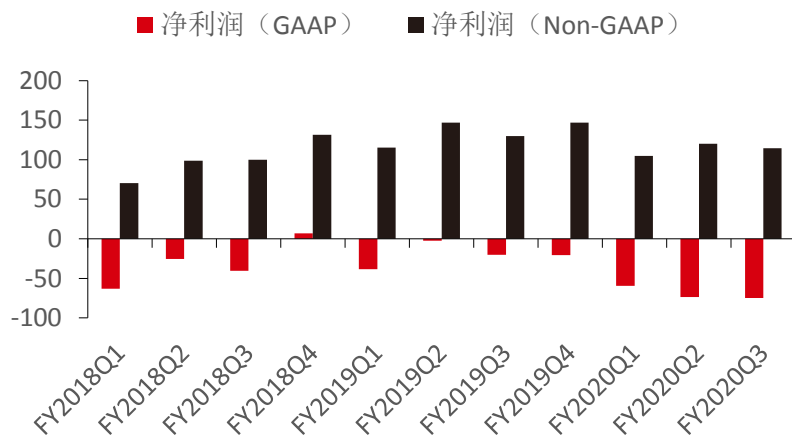
毛利率



费用率



净利润（百万美元）



Palo Alto Networks盈利预测

年度	FY2018	FY2019	FY2020E	FY2021E	FY2022E
营业收入（百万美元）	2,273	2,900	3,379	3,958	4,671
YoY（%）	29%	28%	17%	17%	18%
净利润（GAAP，百万美元）	-148	-82	-235	-100	-73
净利润（Non-GAAP，百万美元）	381	539	475	577	742
YoY（%）	51%	41%	-12%	21%	29%
P/S（x）	10	8	7	6	5

Palo Alto Networks PS band





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

证券研究报告 2020年5月28日

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.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Dalal 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）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.。如对本报告有任何疑问，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。

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。

未经中信证券事先书面授权，任何人不得以任何目的复制、发送或销售本报告。

中信证券2020版权所有。保留一切权利。