计算机

2021 年 03 月 12 日

投资评级：看好（维持）

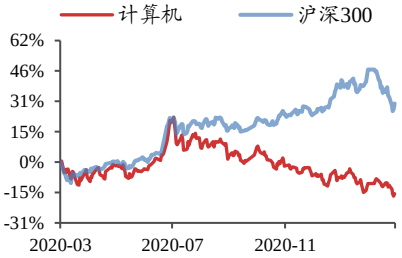
海外网安研究系列之 Palo Alto：“下一代”安全领导者

——行业深度报告

陈宝健（分析师）
chenbaojian@kysec.cn
证书编号：S0790520080001

刘逍遥（分析师）
liuxiaoyao@kysec.cn
证书编号：S0790520090001

行业走势图



数据来源：贝格数据

相关研究报告

《行业周报-周观点：持续看好网络安全板块》-2021.3.7

《行业周报-周观点：2021 年，高度重视网络安全板块》-2021.2.28

《行业周报-周观点：关注超跌的优质标的》-2021.2.21

● 高度看好国内综合实力强，同时在“下一代”安全业务布局领先的厂商

Palo Alto 是下一代防火墙的龙头，于 2005 年成立于美国加利福尼亚州，2007 年，公司首先提出下一代防火墙概念，并推出了第一款下一代防火墙设备 PA-4000，2011-2020 年公司连续 9 年被评选为 Gartner 网络防火墙魔力象限领导者。截至 2021 财年第一季度，公司下一代防火墙已有逾 71000 家客户，年新增客户数达约 8000 家。同时，公司持续加强在云安全、安全运营等方向的投入，实现向“下一代”安全的成功升级。我们认为 Palo Alto 的发展路径实际上对我国专业安全厂商非常具有借鉴意义。高度看好网安领域综合实力强，同时在“下一代”安全业务布局领先的厂商，推荐深信服、奇安信、安恒信息、绿盟科技、启明星辰、美亚柏科，其他受益标的包括天融信、山石网科等。

● Palo Alto 从端到云，安全能力边界不断拓展

公司的发展历程可根据网络安全技术的演变分为三个阶段：2007-2013 年，公司专注于下一代防火墙产品的开发；2013-2017 年，公司在下一代防火墙的基础上转向云安全和端点防护功能的开发；2017 年开始，公司加大投资云与人工智能，发展自动化整体网络安全解决方案。目前，公司已经形成企业安全平台（Strata）、云安全平台（Prisma）和安全运营平台（Cortex）三大安全平台，能够为用户提供从端到云的整体解决方案。

● 下一代安全（Next-Generation Security）成为 Palo Alto 重点发力方向

下一代安全主要包括云安全平台（Prisma）与安全运营平台（Cortex）。（1）云安全平台（Prisma）是针对公有云、与威胁情报云相关的订阅服务集合平台。截至 2021 财年第一季度，Fortune 100 企业中 Prisma Cloud 客户占比达到了 70%，Global 2000 企业中 Prisma Cloud 客户占比为 20%。（2）安全运营平台（Cortex）是与端点防护相关的开放集成的人工智能安全平台。截至 2021 财年第一季度，Cortex 已经完成了超过 400 万个事件的自动化处理，已有 65%的 Fortune 100 企业和 34%的 Global 2000 企业成为了 Cortex 的客户。

● 营收高速增长，订阅收入占比不断提升

（1）2012 财年至 2020 财年，公司营收年复合增速为 38.3%，实现高速增长。（2）得益于公司云平台和安全运营平台业务的快速增长，公司订阅业务收入占比快速提升，到 2020 财年已经达到 69%，成为公司主要收入来源。（3）公司“下一代安全”订单收入增长迅速，在总订单收入中的占比从 13%上升至了 2021 财年第一季度的 24%，是公司未来持续创新与拓展的主要方向。

● 风险提示： 政府及企业 IT 支出缩减；市场竞争加剧；人才流失风险。

目 录

图表目录

1、 从 NGFW 到“下一代”安全，网络安全领导者的成功升级

Palo Alto 于 2005 年成立于美国加利福尼亚州，是全球领先的网络安全服务公司。公司在机器学习、人工智能、自动化与编排等方面持续创新，致力于建设集成的云交付平台与生态系统，为全球的企业、组织、与政府部门等客户在提供着行业领先的网络安全解决方案。

1.1、 下一代防火墙开创者，全球网络安全行业领导者之一

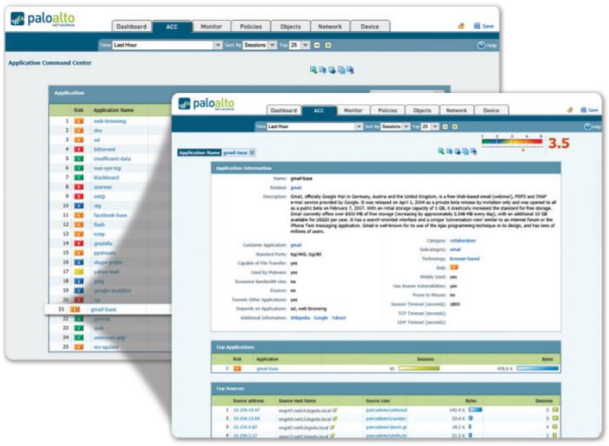
公司的发展历程可根据网络安全技术的演变分为三个阶段：2007-2013 年，公司专注于下一代防火墙产品的开发；2013-2017 年，公司在下一代防火墙的基础上转向云安全和端点防护功能的开发；2017 年至今，公司加大投资云与人工智能，发展自动化整体网络安全解决方案。

1.1.1、 2007-2013：专注下一代防火墙，高筑技术壁垒

公司最初定位是以新一代防火墙为核心的单一网络安全产品厂商。2007 年，公司首先提出下一代防火墙概念，并推出了第一款下一代防火墙设备 PA-4000。下一代防火墙集合了 4 种创新性专利技术，原生集成不同的安全模块，还可根据客户需求添加定制功能。与传统的 UTM 防火墙相比，下一代防火墙具有性能更强、便于管理、应用程序可视等优势。随着系列防火墙设备的推出，公司快速占领下一代防火墙市场。

公司始终围绕着客户需求进行创新，为下一代防火墙添加端点防护等订阅服务，提升竞争优势。2010 年 6 月，公司发布了基于下一代防火墙的远程端点保护服务 GlobalProtect，领先传统 VPN 的数据传输模式获得市场认可；2011 年 11 月，公司又发布了恶意软件检测与分析服务 Wildfire，从被动防御走向主动防御。

图1：下一代防火墙产品可实现应用程序可视化



资料来源：Palo Alto Networks Docs

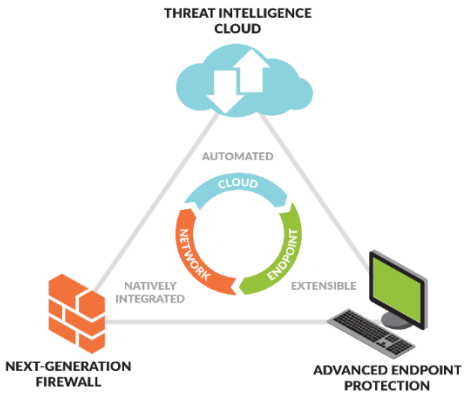
1.1.2、 2013-2017：布局云安全和端点防护，形成三位一体防护体系

随着越来越多的企业将数据中心搬上云端，公司开始重点布局云安全与端点防护。云安全方面，公司于 2013 年便开始在私有云上尝试与 VMware 的整合，于 2014 年正式推出虚拟防火墙 VM 系列，正式实现了在私有云、混合云、和公有云的网络安全服务。**端点防护方面，**公司于 2014 年以 2 亿美元的价格收购了主攻端点防护领域的 Cyvera 公司，在自身的网络安全平台整合了其端点防护功能并命名为 Traps。

Traps 可以通过非签名形式，在用户终端全面防御漏洞与恶意代码攻击。

公司将硬件与软件结合，形成下一代防火墙、云安全、与端点防护三位一体的网络安全平台。通过向脱离实体设备防火墙的云与端点布局，公司帮助客户实现了真正的全平台防御。通过防火墙设备、云端防御、端点防护协同工作，从终端收集数据，识别威胁并自动化生成防御策略，实时推送到各个防御节点。

图2：公司三位一体的防护体系实现全平台防御



资料来源：Palo Alto Networks

1.1.3、 2017 至今：投资云与人工智能，加强整体信息安全防护解决方案

随着产业技术升级，客户需求复杂化，公司开始致力于为客户提供整体信息安全解决方案。公司于 2018 年推出了云应用框架（Application Framework），以 SaaS 模式为客户提供了自动、连续、可扩展的云交付功能，并为第三方提供了快速产品开发和交付的安全生态平台。2019 年 2 月，公司将云应用框架全面变革升级为基于人工智能的持续安全平台 Cortex，引入人工智能与机器学习技术，加强整体网络安全平台性能。

图3：云应用框架为客户提供了云交付的一体化解决方案

资料来源：Palo Alto Networks Blog

公司加大在人工智能、机器学习、自动化方向的投资，不断提升产品与服务竞争力。公司持续进行兼并收购，收购对象为在云和人工智能的某些细分领域拥有突出技术优势的初创企业。公司目前的多个服务都集合了以往收购企业的技术，例如 Prisma Cloud 整合了 Evident.io、Redlock、Twistlock、PureSec 和 Aporeto 的技术，Prima Saas 整合了 Aperture 的技术，Cortex XSOAR 则整合了 Demisto 的技术。公司

通过在自身网络安全平台上整合这些行业前沿的新技术，加强了在云环境下的安全能力，保持了市场竞争力。在公司对 2021 财年的总订单收入预测中，约 15%的收入贡献来自公司自 2019 年以来收购的企业。

表1：2017 年以来公司加大云与人工智能方向投资（单位：百万美元）

宣布日期	目标公司	收购金额	公司核心优势
2017 年 2 月 28 日	Light Cyber Ltd	105	自动化威胁检测
2018 年 3 月 14 日	Evident.io Inc	300	云安全
2018 年 4 月 10 日	Secdo Ltd	100	端点防护
2018 年 10 月 3 日	Redlock Inc	173	云安全
2019 年 2 月 19 日	Demisto Inc	560	编排和自动化安全技术
2019 年 5 月 29 日	Puresec Ltd	47	无服务器安全平台
2019 年 5 月 29 日	Twistlock Ltd	410	容器安全
2019 年 9 月 4 日	Zingbox Ltd	75	物联网安全
2019 年 11 月 25 日	Aporeto Inc	150	微服务云安全
2020 年 3 月 31 日	CloudGenix Inc	420	软件定义广域网
2020 年 8 月 24 日	Crypsis Group Holdings LLC	265	安全事件响应
2020 年 11 月 11 日	Expanse Inc	800	攻击面管理
2020 年 11 月 19 日	Sinefa Group Inc	44	数字体验监控

资料来源：Palo Alto Networks Press Release、开源证券研究所

1.2、 防火墙龙头地位稳固，潜在市场空间广阔

1.2.1、 连续九年评为 Gartner 魔力象限领导者，获得市场长期高度认可

多次获得行业权威机构认证，行业领导者地位稳固。2020 年 Gartner 网络防火墙魔力象限评比中，公司在前瞻性和执行能力两个方面都达到了行业第一。2011-2020 年公司连续 9 次被评选为 Gartner 网络防火墙魔力象限领导者。2015-2020 年，公司连续 6 次被技术服务行业协会（TSIA）评为“卓越”，并且连续 6 次获得 JD Power 的全球辅助技术支持的“卓越客户服务体验”认证。

图4：公司连续 9 次被评为 Gartner 网络防火墙魔力象限领导者

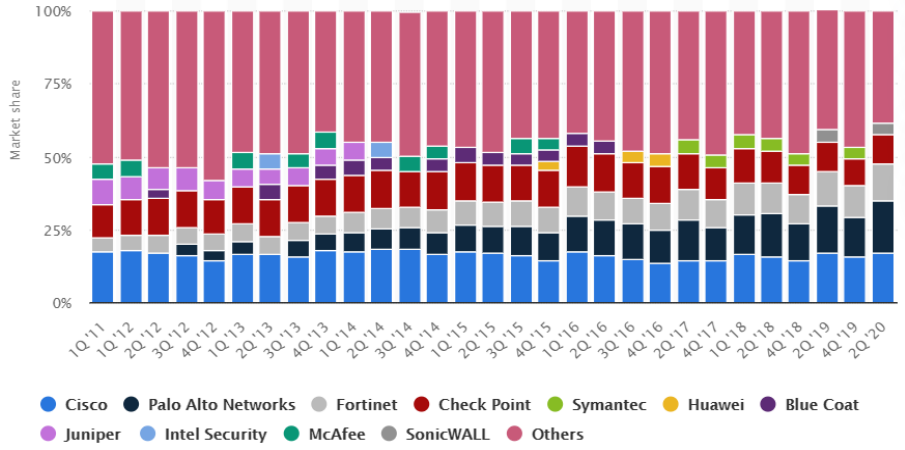
资料来源：Gartner

图5：公司 2020 年第 6 次获得杰出辅助技术支持认证

资料来源：Palo Alto Networks

公司在信息安全设备市场份额持续稳步上升。根据 Statista 数据，公司在信息安全设备市场的市场份额逐年上升。

图6：2011 年至 2020 年全球信息安全设备市场中公司市场份额逐年扩大



资料来源：Statista

2020 年第二季度公司在全球网络安全设备市场份额居首。根据 IDC 的统计，公司在网络安全设备领域的市场份额已于 2020 年第二季度超过其最大的竞争对手 Cisco。2020 年第二季度公司市场份额为 18.1%，全球排名第一。

表2：2020Q2 公司在全球网络安全设备市场的份额居首位（单位：百万美元）

公司	2020Q2 营收	2020Q2 市场份额	2019Q2 营收	2019Q2 市场份额
1. Palo Alto Networks	759.4	18.1%	633.7	16.3%
2. Cisco	711.4	17.0%	660.8	16.9%
3. Fortinet	534.4	12.7%	452.9	11.6%
4. Check Point	420.0	10.0%	405.2	10.4%
5. SonicWALL	164.1	3.9%	158.8	4.1%
其他	1604.1	38.3%	1587.8	40.7%
合计	4193.4	100%	3899.3	100%

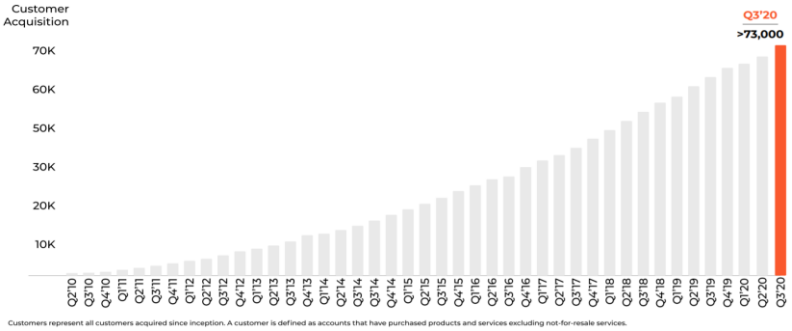
数据来源：IDC、开源证券研究所

1.2.2、 渠道合作伙伴计划 NextWave 激励效果明显，客户基数稳定增长

NextWave 计划实现公司与渠道合作伙伴共同盈利。公司产品与服务的销售模式一般为：公司→分销商→经销商→终端客户，因此公司非常重视对接客户的渠道业务。为激励分销商和经销商为公司带来更多商机并保障为客户提供的服务质量，公司推出了合作伙伴项目 NextWave。该项目一方面为合作伙伴提供技术和销售等培训，使合作伙伴能够为客户提供专业而完善的售前、售后、及托管服务。另一方面设计合理激励的盈利方案，依据合作伙伴报备的数量、产生的商机、带来的订单和新客户增加数量等评估指标将合作伙伴分为三个等级——创新者（Innovator）、铂金（Platinum）、与钻石（Diamond），并根据不同等级给予不同的奖励措施，使合作伙伴能够持续为公司带来新客户，实现共同盈利。

分销收入对公司营业总收入贡献高，获客数量稳定增长。2020 财年，公司已有逾 5,600 家合作分销商与经销商，有 4 家合作分销商贡献了 23.45 亿美元的营业收入，占总营收的 68.8%。截至目前，公司的客户数量已逾 77,000 家，遍布全球 170 多个国家和地区，覆盖约 85%的 Fortune 500 强企业。

图7：公司客户数量持续增长



资料来源：Palo Alto Networks FY2020Q3 投资者演示材料

1.2.3、 潜在市场规模大，未来仍有很大增长空间

Gartner 预测 2022 年全球信息安全领域潜在市场规模可达 726 亿美元，2018 年至 2022 年的复合增长率可达 9.2%。其中，云端服务的潜在市场规模年复合增长率最快，达到 21.2%。云、端点防护、安全运维自动化将是公司未来发展的关键点。

图8：2022 年全球信息安全领域潜在市场规模预计可达 726 亿美元

资料来源：Palo Alto Networks FY2020Q3 投资者演示材料

2、 业务分析：产品线丰富，整体解决方案行业领先

从品牌战略的角度，公司将产品线划分至三大平台：企业安全平台（Strata）、云安全平台（Prisma）和安全运营平台（Cortex）。

图9：三大产品平台为客户提供全方位网络安全解决方案

资料来源：Palo Alto Networks

2.1、 企业安全平台（Strata）提供业内领先的网络安全套件

企业安全平台（Strata）是以下一代防火墙设备为基础的产品组合平台。该平台下主要有下一代防火墙、相关订阅服务和网络安全管理工具 Panorama。（1）下一代防火墙可以多种形式部署，包括实体防火墙 PA 系列、虚拟防火墙 VM 系列，和容器防火墙 CN 系列。（2）相关订阅服务附加于下一代防火墙，目前一共有 8 种，包括 2007 年至 2011 年推出的 Threat Prevention、URL Filtering、Global Protect 和 WildFire，还有 2019 年至 2020 年推出的 DNS Security、SD-WAN、DLP 和 IoT。网络安全管理工具 Panorama 可以硬件或软件形式部署，对公有云和私有云进行防护。

表3：企业安全平台（Strata）产品线完善

产品类型	产品名称	介绍
新一代防火墙	物理设备（PA-Series）	新一代防火墙物理设备种类齐全，易于部署到组织网络中。它经过专门设计，简单易用、可自动化且可集成。
	虚拟防火墙（VM-Series）	虚拟新一代防火墙通过分段和威胁防御，保护私有云和公有云部署的安全。
	容器防火墙（CN-Series）	对容器信任区域和其他工作负载类型之间的入站、出站和东西向流量提供威胁防护，同时不拖慢开发速度。
安全产品订阅	威胁防御（Threat Prevention）	2007 年推出，威胁防御可以一次扫描即可阻止已知的客户端和服务器端漏洞利用、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 过滤（URL Filtering）	2007 年推出，URL 过滤可以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。可保护组织免受各种安全、法律、法规、合规和可接受使用风险的侵害，并与 WildFire 共享威胁数据。
	GlobalProtect	2010 年推出，GlobalProtect 提供强大的威胁防御功能，保护用户免受恶意应用流量、网络钓鱼、凭证盗窃等侵害。同时能对移动用户提供新一代防火墙的保护。
	WildFire	2011 年推出，WildFire 可以检测并防止未知攻击，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	2019 年推出，DNS Security 使用预测分析、机器学习，和自动编排阻止利用 DNS 发动的攻击。通过与公司新一代防火墙紧密集成提供自动防护。
	SD-WAN	2019 年推出，SD-WAN 将安全性与 SD-WAN 结构本地化结合，保障分支机构的连接安全。
	企业数据丢失防护（DLP）	2020 年推出，作为云服务，Enterprise DLP 解决方案能够发现、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。
	物联网安全（IoT Security）	2020 年推出，业内首个物联网安全解决方案，利用机器学习和 App-ID 技术，可以准确地识别各种不受管制的设备、确定正常行为的基准、识别异常活动、评估风险并提供策略建议。
网络安全管理	Panorama	集中式安全管理解决方案，是用于全局控制而部署在终端客户网络上的防火墙设备和软件，以及公共或私有云环境中作为虚拟设备或物理设备部署的防火墙设备和软件。Panorama 用于集中式策略管理、设备管理、软件许可和更新、集中式日志记录和报告，以及日志存储。

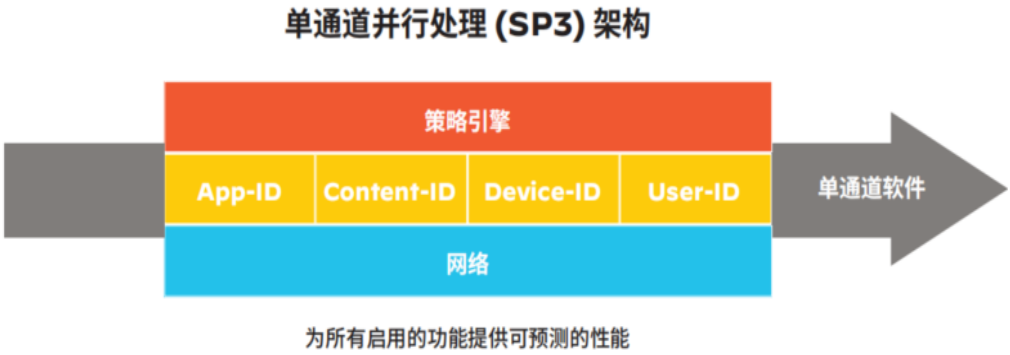
资料来源：Palo Alto Networks、开源证券研究所

2.1.1、 下一代防火墙具备四大独特技术，形成强技术壁垒

区别于传统的统一威胁管理（UTM）平台，公司的下一代防火墙依靠四项自其 2007 年诞生以来便具备的独特技术：App-ID、User-ID、Content-ID 和单通道并行处理体系结构，满足了客户在复杂环境下的网络安全需求。2020 年 7 月，公司发布

了最新的下一代防火墙运行系统版本 PAN-OS 10.0，其中的 IoT 订阅服务带来了设备识别技术 Device-ID。多种技术的结合，共同树立了下一代防火墙强大的技术壁垒。

图10：多种技术结合为下一代防火墙筑造强大技术壁垒



资料来源：Palo Alto Networks

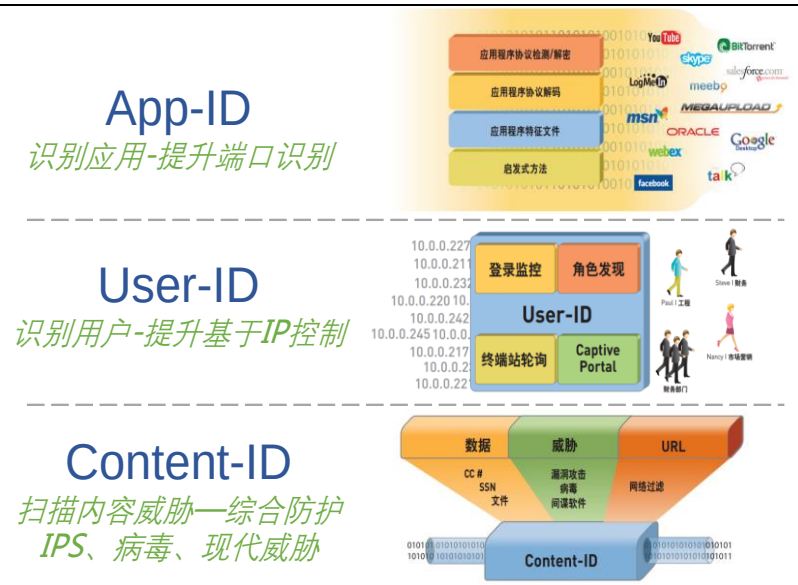
- **App-ID、User-ID、和 Content-ID 技术为核心**

App-ID 是一种先进的流量精确分类机制，实现了对应用程序的识别、可视性及控制。区别于传统防火墙基于端口和协议的流量分类机制，它可以在设备检测到流量后判断传输数据的具体应用程序身份，无论该应用程序是否透过网页服务、SSL 加密或其他规避技术，从而突破了传统防火墙的流量分类限制。

User-ID 实现了使用者层级的可视性与控制。通过与 Microsoft AD 的无缝整合，下一代防火墙可以动态对应 IP 地址和用户，还可以针对用户进行政策制定，从而控制用户对应用程序的使用。

Content-ID 具备的技术组件实现了预防流量中的威胁、提供可视性，和文件与数据筛选功能。威胁预防组件提供了入侵监测和防御功能；网址过滤组件提供了海量高度整合、可定制化的网址过滤资料库；文件与数据筛选组件同时利用 App-ID 的深层应用程序检查功能，实现了对敏感数据传输的阻挡。

图11：三大识别技术是下一代防火墙的核心

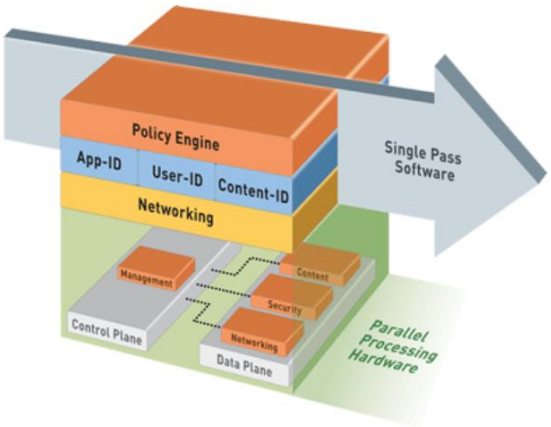


资料来源：Palo Alto Networks Docs、开源证券研究所

➢ **单通道并行处理体系结构为基础**

单通道并行处理体系结构的两个关键要素是单通道软件体系结构和自定义构建的并行处理硬件平台。下一代防火墙通过独特的硬件与软件集成方法，简化了流程管理，极大地提高了性能。

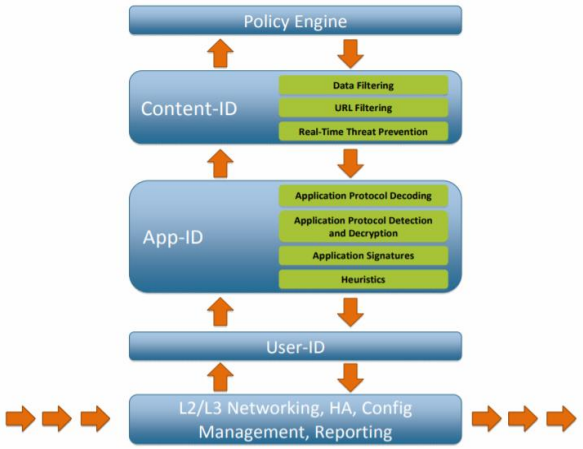
图12：单通道并行处理体系结构是下一代防火墙的基础



资料来源：Palo Alto Networks Docs

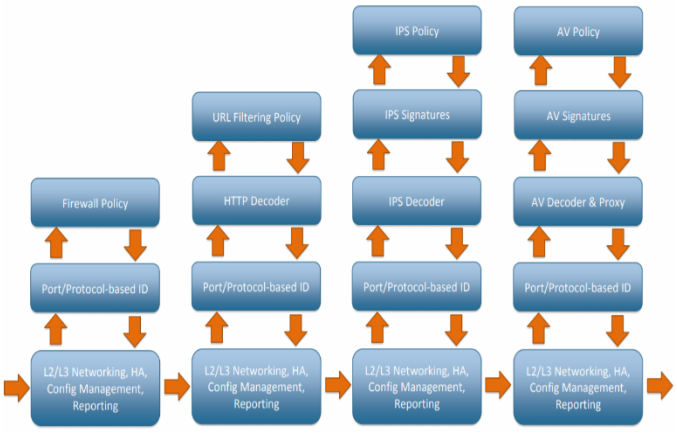
单通道软件体系结构助力下一代防火墙性能快速提升。传统防火墙产品大多使用的是多通道、多模组、多管理系统的 UTM 平台。该类平台的安全引擎只是简单拼接在了一起，数据处理流仍需在每个安全引擎分别执行解码、状态复原等操作，消耗大量资源。而下一代防火墙采用的单通道软件结构可以一次性同时进行多种检测，在处理数据包时可以同时执行联网功能、策略查找、应用程序识别和解码等任务，因此更加适合大型企业。

图13：单通道软件结构的数据包可一次性快速处理



资料来源：Palo Alto Networks Docs

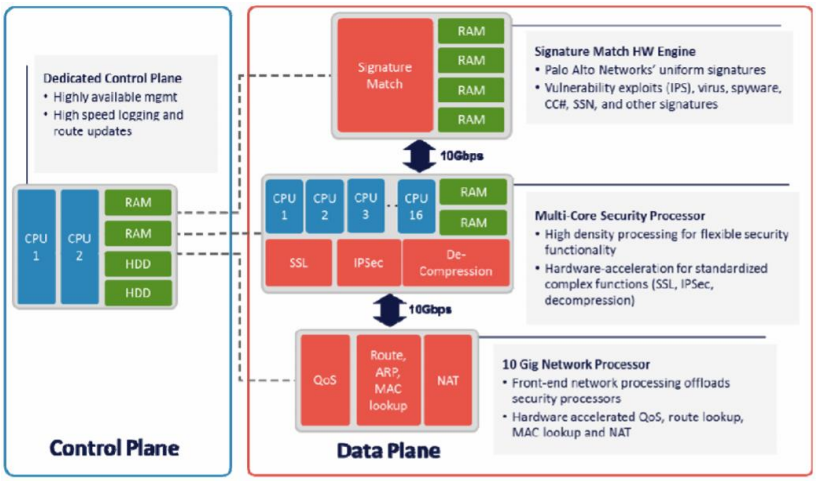
图14：多通道硬件结构的数据包需多次解码复原



资料来源：Palo Alto Networks Docs

并行处理硬件平台确保了下一代防火墙整体运行的稳定性。并行处理架构结合了数据板块（Data Plane）和控制板块（Control Plane）两部分，以此来实现硬件层面的特定功能。数据和控制板块依靠其各自的 CPU 和 RAM 独立运行，互不影响。因此避免了单个板块性能波动对平台整体运行的影响，确保稳定性。

图15：数据板块与控制板块互相独立运行



资料来源：Palo Alto Networks Docs

2.1.2、 下一代防火墙产品系列完善，客户稳定增长

下一代防火墙经过多年发展目前分为实体防火墙 PA 系列、虚拟防火墙 VM 系列、容器防火墙 CN 系列。（1）**PA 系列**针对客户的不同性能要求而设计，并根据吞吐量大小分类，有适用于企业分支机构的 PA-200，也有适用于大规模数据中心和服务商的 PA-7080。（2）**VM 系列**应用于虚拟和云环境，支持 VMware、Microsoft、Amazon、Google、KVM／Openstack 环境。它可以提供与硬件设备相同的高级威胁防御功能，保护公有云、虚拟和 NFV 环境中部署的应用和数据安全。（3）**CN 系列**是 2020 年在基于机器学习的下一代防火墙版本 PAN 10.0 上推出的容器防火墙，可以将防火墙部署直接集成到 DevOps 工作流中，专门为 Kubernetes 环境构建。

图16：实体防火墙 PA 系列产品型号多样

资料来源：Palo Alto Networks

部署下一代防火墙的客户数量稳定增长。截至 2021 财年第一季度，下一代防火墙已有逾 71,000 家客户，年新增客户数达 8,000 家。其中软件防火墙（虚拟防火墙 VM 系列和容器防火墙 CN 系列）已有逾 10,000 家客户，年新增客户数达约 2,500 家。

2.2、 云安全平台（Prisma）提供业内最全面的云安全产品

云安全平台（Prisma）是针对公有云、与威胁情报云相关的订阅服务集合平台。云安全平台下的产品套件有云原生安全平台 Prisma Cloud、云交付式移动用户安全服务 Prisma Access、和保护 SaaS 访问安全服务 Prisma SaaS。其中，Prisma Access 和 CloudGenix SD-WAN 相结合，组成了业内最全面的安全访问服务边缘 SASE（Secure Access Service Edge），为用户提供具有云交付安全功能的全球云网络。

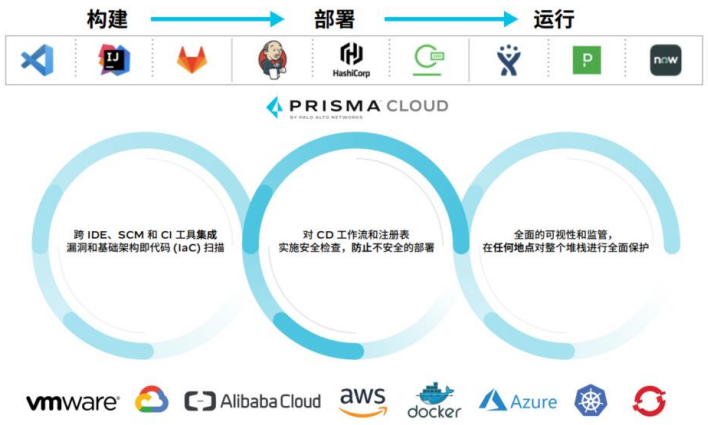
表4：云安全平台（Prisma）产品线完善

产品类型	产品名称	介绍
云原生架构平台	Prisma Cloud	在整个云原生技术堆栈中启用一套集成的安全功能，且在多云和混合云环境中保持一致的安全和合规管理，并能识别和防御威胁以及异常活动。
云交付网络安全	Prisma Access	专为安全访问服务边缘 (SASE) 设计，Prisma Access 在专门构建的云交付基础架构中提供组织所需的网络和安全性。它使用一种通用的基于云的基础架构，可以从全球 76 个国家/地区的 100 多个地点提供防护，为所有应用提供网络和一致的安全性，确保始终执行相同的策略。
	Prisma SaaS	可为所有应用提供一致化的高级数据保护，控制数据公开、泄露及不合规风险。可以解决云访问安全代理需求并提供有关风险监测、数据丢失防护、合规性保障、数据监管、用户行为监控和高级威胁防护的高级功能。
	CloudGenix SD-WAN	业内第一个允许云交付分支机构的 SD-WAN。通过深层的应用程序可见性和智能的 7 层网络策略、机器学习和数据科学，减少云交付分支机构的网络安全成本。

资料来源：Palo Alto Networks、开源证券研究所

疫情催化下企业加速数字化转型，Prisma Cloud 需求快速上升。受新冠疫情下远程办公需求影响，企业加速将数据中心和服务上云，Prisma Cloud 订阅量大幅上升。目前，Prisma Cloud 已为逾 18 亿的云上资源保驾护航。截至 2021 财年第一季度，Fortune 100 企业中 Prisma Cloud 客户占比达到了 70%，这一比重在 2020 财年第三季度为 43%；Global 2000 企业中 Prisma Cloud 客户占比为 20%，这一比重在 2020 财年第四季度为 14%。

图17：Prisma Cloud 可在全生命周期、全堆栈、任何云提供安全与合规覆盖



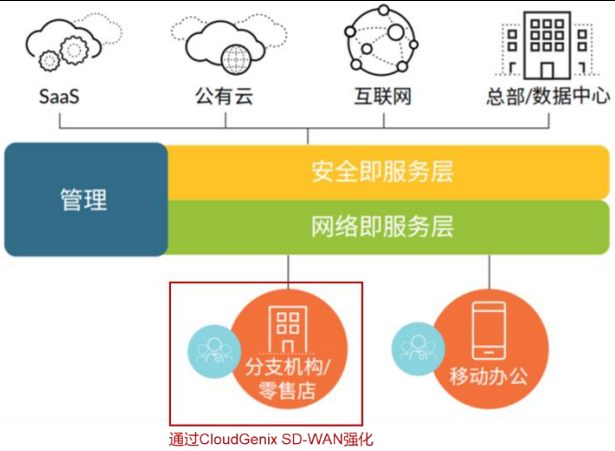
资料来源：Palo Alto Networks

Prisma Access 成为业界最全面安全访问服务边缘平台。Prisma Access 是一种安全访问服务边缘（SASE）解决方案，原名为 GlobalProtect 云服务。Prisma Access 利用了云交付的通用基础架构，用户只需连接到 Prisma Access，便可以安全使用 SaaS、公有云、互联网、及数据中心。通过部署 Prisma Access，用户不再需要部署实体防火

墙。2020 年 10 月 13 日，公司发布了 Prisma Access 2.0，它通过与 CloudGenix SD-WAN 技术的结合，实现了对分支机构安全服务的强化，使 Prisma SASE 成为了业界最全面的 SASE 平台。

疫情期间，居家办公的方式带来了 Prisma SASE 客户的大量增长，很多客户通过 Prisma Access 的免费试用转化成为了付费用户。截至 2021 财年第一季度，已有逾 1000 名客户订阅 Prisma SASE 服务，年增长率大于 100%。

图18：Prisma Access 为远程网络和移动用户提供一致的安全功能



资料来源：Palo Alto Networks、开源证券研究所

2.3、 安全运营平台（Cortex）提供业内最全面的安全运营产品套件

安全运营平台（Cortex）是与端点防护相关的开放集成的人工智能安全平台。Cortex 是云应用框架的升级，由 Cortex Data Lake 驱动，聚焦于深度挖掘和分析，致力于发现潜在威胁和未知攻击手段，以及攻击溯源、自动化响应流程等，为企业提供一流的检测、调查、自动化和响应能力。Cortex 平台下有扩展的检测与响应套件 Cortex XDR、扩展的安全编排、自动化和响应平台 Cortex XSOAR、专为安全分析创建的优质数据湖 Cortex Data Lake、和情景威胁情报服务 AutoFocus。

表5：安全运营平台（Cortex）功能完善

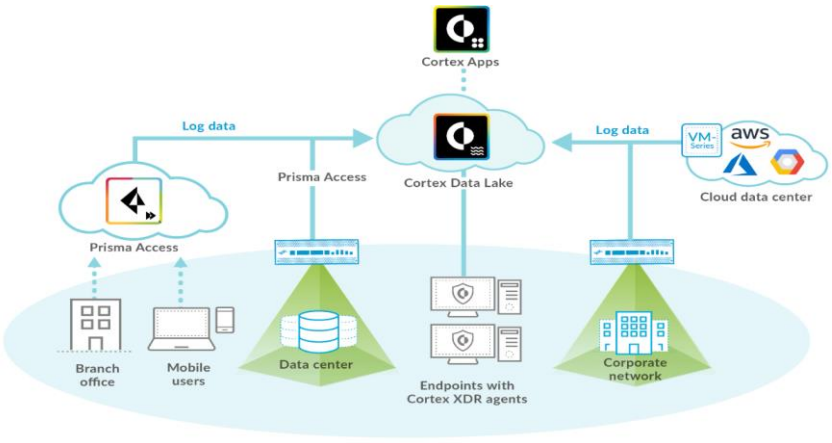
产品名称	介绍
Cortex XDR	在整个云原生技术堆栈中启用一套集成的安全功能，且在多云和混合云环境中保持一致的安全和合规管理，并能识别和防御威胁以及异常活动。
Cortex XSOAR	一种综合安全编排、自动化和响应 (SOAR) 平台，能够统一案例管理、自动化、实时协作和威胁情报管理，在整个事件生命周期内为安全团队提供支持。
Cortex Data Lake	通过对终端、网络和安全设备日志等数据的收集而形成的数据湖。它采用将企业数据规范化并拼接在一起的方法，获取公有云规模和位置，保障数据安全和隐私。通过数以万亿计的多源分析项目，大幅提高安全成果的准确性。
AutoFocus	威胁情报服务能够针对破坏力最强、最具有针对性的特殊攻击提升威胁分析与追踪工作流的速度。其托管式安全服务可扩展公司安全平台所需的可见性和威胁上下文信息，无需添加额外的 IT 安全资源，实现对重大攻击更快速的响应。

资料来源：Palo Alto Networks、开源证券研究所

Cortex 平台广获客户青睐。Cortex 的自动化防御功能每天自动化处理逾 1 百万个已知威胁，为客户减少了 95%的威胁警报。截至 2021 财年第一季度，Cortex 已经完成了超过 400 万个事件的自动化处理，数量在四个月内增加了 100%。已有 65%的

Fortune 100 企业和 34%的 Global 2000 企业成为了 Cortex 的客户。

图19：Cortex 收集端点数据至数据湖后进行自动分析处理



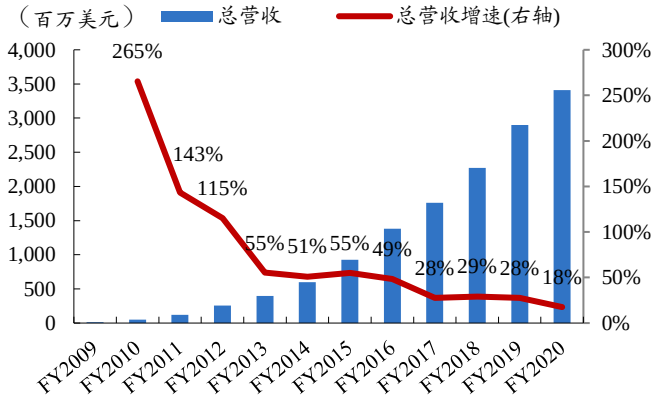
资料来源：Palo Alto Networks Blog

3、 财务分析：营收高速增长，订阅收入占比不断提升

3.1、 主营业务收入快速增长，疫情之下订单收入仍保持高速增长

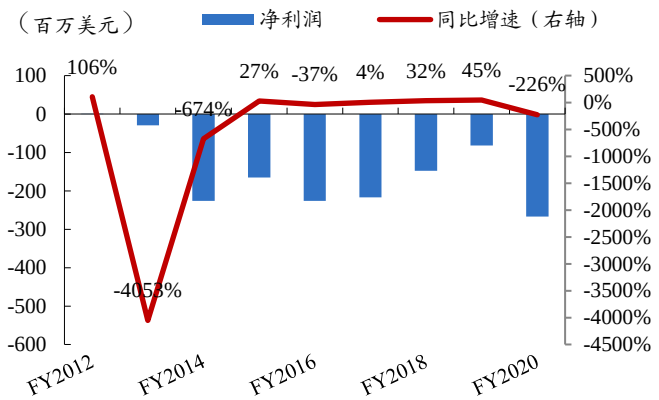
公司主营业务收入始终保持着快速增长。2012 财年至 2020 财年，公司营收年复合增速为 38.3%。2020 财年总营收 34.08 亿美元，同比增速略有下降，主要原因是新冠疫情导致实体防火墙部署需求有所下降，相应产品销售收入下降。净利润在 2017 财年至 2019 财年间亏损逐步缩小，公司盈利能力好转。2020 财年公司亏损再次扩大原因为研发支出的大幅上升，此外，公司还计划在 2020 财年后的 2.5 年内以直线摊销法确认 15 亿美元的股权激励费用，将对净利润状况有所影响。

图20：FY2017 以来公司营业收入增长稳定



数据来源：Wind、开源证券研究所

图21：FY2017 以来净利润状况较为波动

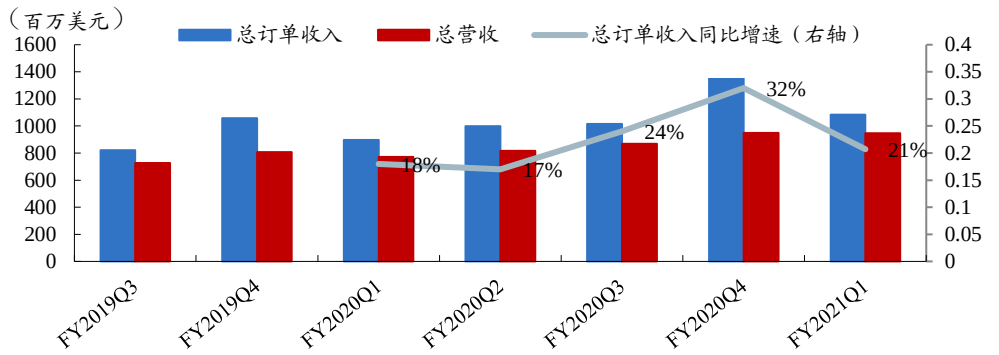


数据来源：Wind、开源证券研究所

公司总订单收入同比增速保持增长，受疫情影响较小。总订单收入（total billings）是判断公司经营健康状况的另一重要指标，在总营业收入（total revenue）基础上加入了总递延收入变动（change in total deferred revenue）和新增递延收入净额（net of acquired deferred revenue）。递延收入主要由订阅与支持服务的订单收入构成，客户通常选择一次性为这些合同期为一年以上的 SaaS 服务支付费用，而营业收入的确认需要在各服务对应的合同期内才能完成。2020 财年第四季度和 2021 年第一季度，公司

总订单收入分别达到 13.9 亿美元和 10.83 亿美元，同比增长率分别为 32%和 21%，在疫情影响下公司业务仍保持了高速增长。

图22：FY2019Q3-FY2021Q1 公司总订单收入保持高速增长



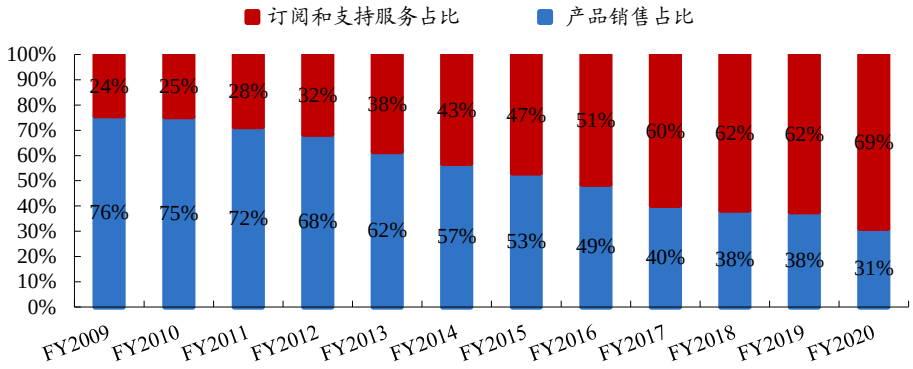
数据来源：Palo Alto Networks 2020 财年第三、四季度和 2021 财年第一季度 Earning Call 演示材料、开源证券研究所

3.2、 订阅收入占比快速提升，下一代安全业务高速增长

3.2.1、 财务报表角度拆分：订阅与支持服务占比快速提升，成为主要收入来源

订阅与支持服务收入成为主要收入来源。公司财务报表将主营业务收入划分为产品销售收入和订阅与支持服务收入。产品销售主要包括防火墙设备的销售，订阅和支持服务收入包括新客户购买的基于防火墙以及独立提供的订阅与支持服务，还有老客户的续订和支持服务。2009 财年至 2020 财年，订阅与支持服务销售收入占比持续上升，于 2016 财年超过产品销售收入占比，2020 财年已达到 69%，成为公司营收主要组成部分。

图23：FY2009 以来公司订阅与支持服务销售额占总营收比重持续扩大



数据来源：Wind、开源证券研究所

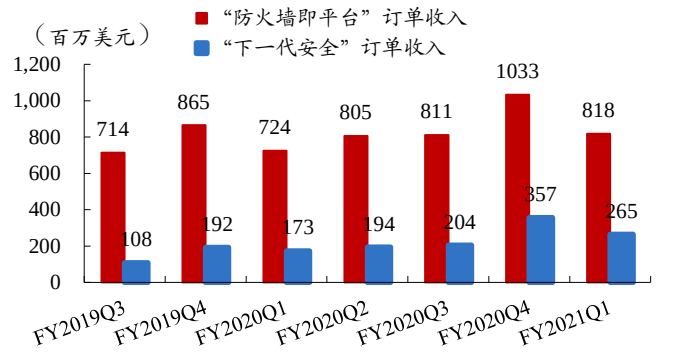
3.2.2、 公司业务角度拆分：下一代安全业务收入高速增长

2019 年开始，公司将总订单收入分为了两部分：防火墙即平台（Firewall-as-a-Platform，简称 FwaaP）和下一代安全（Next-Generation Security，简称 NGS）。（1）“防火墙即平台”即公司的下一代防火墙业务，该部分订单收入包括了实体防火墙、虚拟防火墙相关订阅与支持服务、Prisma Access（属软件防火墙）及 CloudGenix 的订单收入。（2）“下一代安全”部分的订单收入则包括了云安全平台（Prisma）与安

全运营平台（Cortex）套件订单，以及虚拟防火墙订单所贡献的收入。

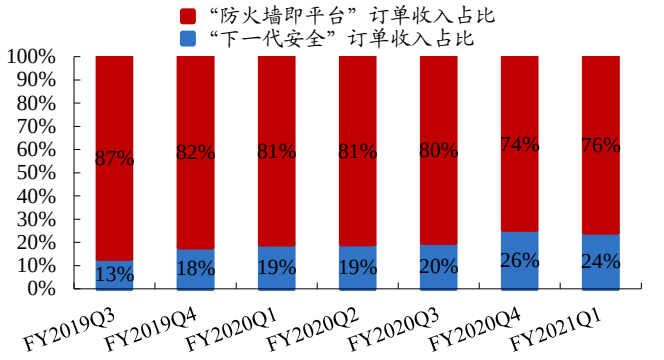
“下一代安全”业务高速增长。2019 财年第三季度到 2021 财年第一季度，“下一代安全”订单收入增长迅速，在总订单收入中的占比从 13%上升至了 2021 财年第一季度的 24%，是公司未来持续创新与拓展的主要方向。

图24：FY2019Q3 以来“下一代安全”订单收入增长迅速



数据来源：Palo Alto Networks 2021 财年第一季度 Earning Call 演示材料、开源证券研究所

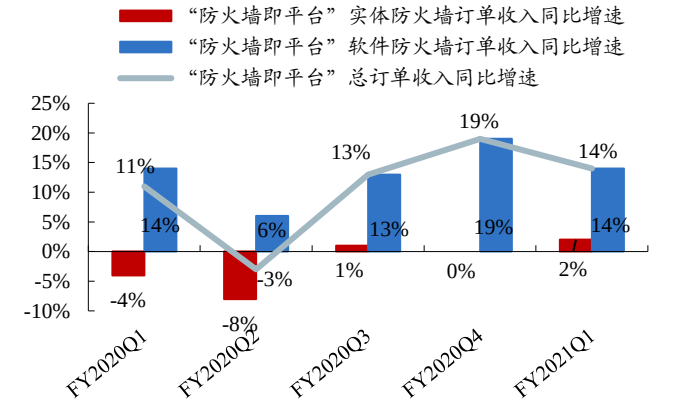
图25：FY2019Q3 以来“下一代安全”占比快速上升



数据来源：Palo Alto Networks 2021 财年第一季度 Earning Call 演示材料、开源证券研究所

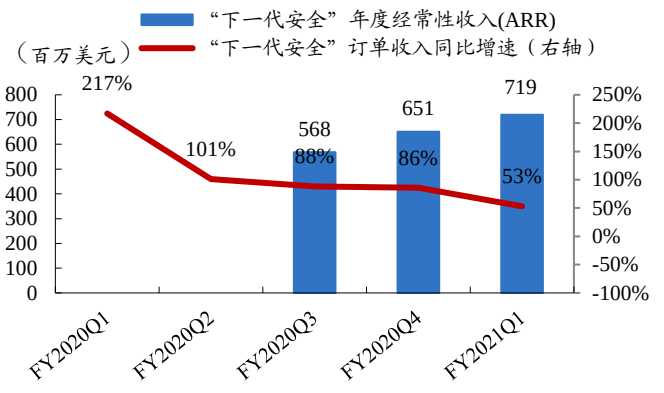
软件防火墙订单收入正增长，“下一代安全”SaaS 业务快速增长。根据公司披露的数据，2020 财年第一季度至 2021 财年第一季度，“防火墙即平台”业务中，实体防火墙订单收入增长陷入停滞，平均同比增速为-1.8%；而软件防火墙（包括 Prisma Access 与 CloudGenix SD-WAN）订单收入实现较快增长。“下一代安全”业务订单收入相比“防火墙即平台”则保持着高速增长，其中 SaaS 服务的年度经常性收入（ARR）从 2020 财年第三季度的 5.68 亿美元增长至 2021 财年第一季度的 7.19 亿美元，表明云安全平台（Prisma）和安全运营平台（Cortex）产品受到客户认可和欢迎。

图26：FY2020Q1 以来公司软件防火墙快速增长



数据来源：Palo Alto Networks 2021 财年第一季度 Earning Call 演示材料、开源证券研究所

图27：FY2020Q1 以来“下一代安全”业务高速增长



数据来源：Palo Alto Networks 2021 财年第一季度 Earning Call 演示材料、开源证券研究所

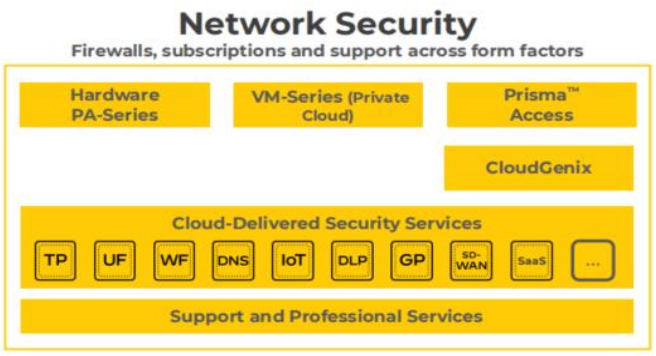
2021 财年第一季度，公司将原先划分的两大业务微调并重新定义为“网络安全”和“云与人工智能”。公司在“防火墙即平台”业务中加入相关订阅、支持、与专业服务，并称之为“网络安全（Network Security）”。公司在“下一代安全”业务中移除了私有云虚拟防火墙以避免重复计算，并称之为“云与人工智能（Cloud&AI）”，该板块代表公司未来的重点发展方向。

“网络安全”板块是业内最大的防火墙业务，并且将持续增长。公司披露，2020

财年全年“网络安全”业务营收达 30.9 亿美元，占总营收的 90.7%。据 Gartner 于 2020 财年第二季度的统计，公司“网络安全”板块是企业网络设备市场份额最大的防火墙业务。在软件防火墙替代实体防火墙增长的趋势下，公司预测 2021 财年该板块将迎来 14%的年增长率，取得 35.1 亿美元营收。

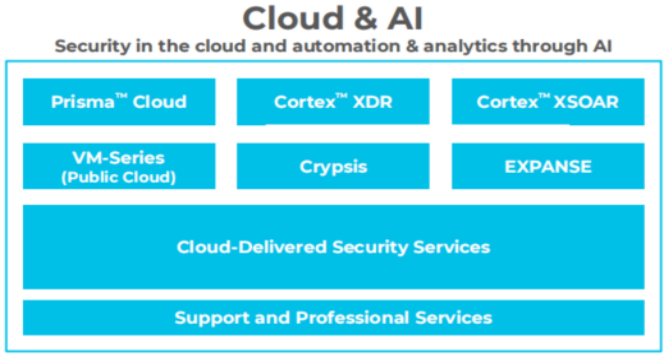
“云与人工智能”板块随获客数量增加，未来将继续高速增长。公司披露，2020 财年全年“云与人工智能”业务营收达 3.18 亿美元，占总营收的 9.3%；年度经常性收入（ARR）达 3.88 亿美元。公司预测 2021 财年，该板块营收和 ARR 分别将获得 90%和 89%（其中 18%来自 Expanse）的高增长率，分别达到 6.05 亿美元和 7.35 亿美元。企业网络安全转型是数字化转型安全的保障，我们认为未来随着企业加快数字化转型，公司获客数量上升，“云与人工智能”板块的业绩将持续高速增长。

图28：“防火墙即平台”+相关服务=“网络安全”



资料来源：Palo Alto Networks 2021 财年第一季度 Earning Call 演示材料

图29：“下一代安全”-私有云防火墙 =“云与人工智能”

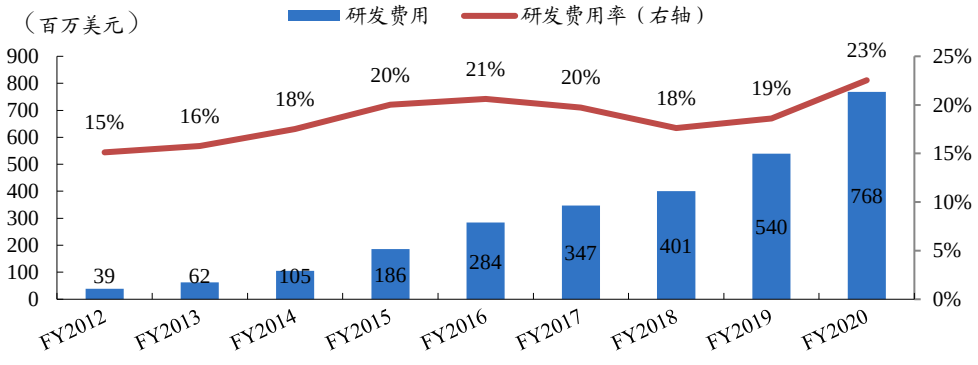


资料来源：Palo Alto Networks 2021 财年第一季度 Earning Call 演示材料

3.3、 研发投入近年加大，销售与管理费用率逐步下降

近年来公司再次加大研发投入，2018 财年至 2020 财年研发费用率持续上升。2020 财年公司研发费用达到 7.68 亿美元，占营收的 23%，为公司上市以来最高水平。未来公司将继续加大研发投入，持续产品创新。

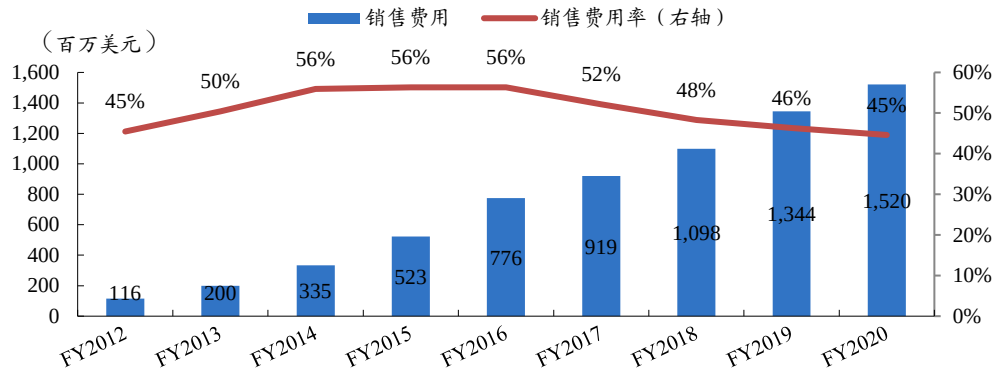
图30：近三个财年研发费用率持续上升



数据来源：Wind、开源证券研究所

以 2016 财年为拐点，销售费用率逐渐下降。销售费用主要包括人员成本和佣金费用等，自上市以来一直占营收 45%以上，反映出公司对营销的重视。公司规模效应于 2016 年显现，获客成本降低带来销售费用率的下降。

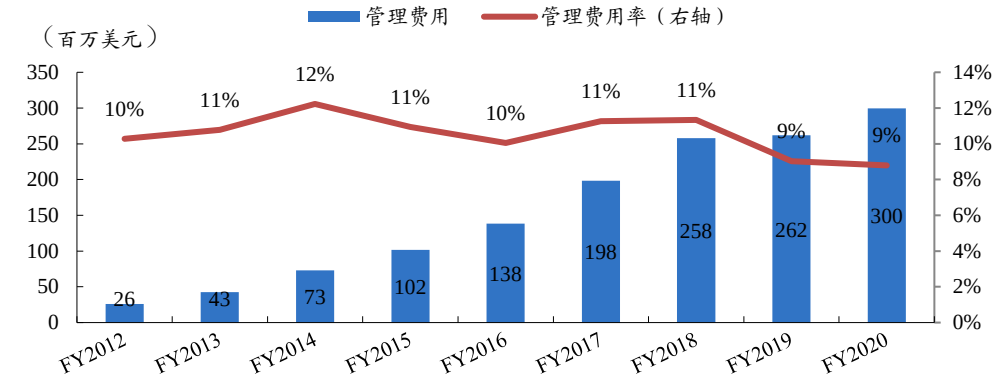
图31：销售费用率自 2016 财年逐步下降



数据来源：Wind、开源证券研究所

公司管理费用率近三年呈下降趋势。2012 财年以来，公司管理费用率始终在 10%上下波动。2018 财年至 2020 财年，公司管理效率提升，管理费用率呈下降趋势。

图32：近三个财年公司管理费用率呈下降趋势



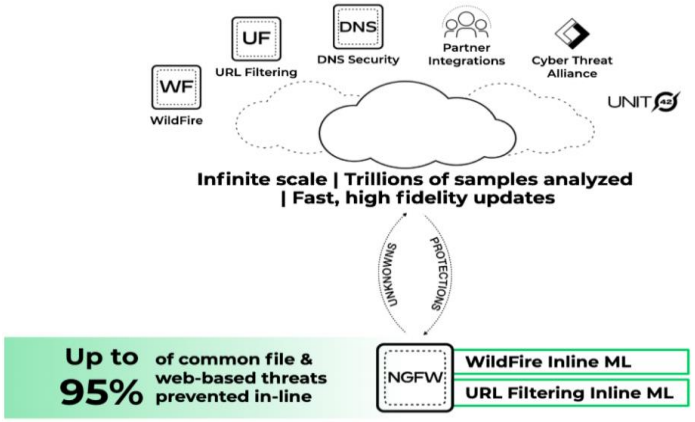
数据来源：Wind、开源证券研究所

4、 未来发展方向：机器学习技术与 5G

4.1、 为下一代防火墙嵌入机器学习技术，强化性能

未来公司将继续在机器学习、人工智能等方向加大投入。2020 年 6 月 17 日，公司正式发布了业界第一款基于机器学习的下一代防火墙版本 PAN-OS 10.0。该更新版本将机器学习技术嵌入防火墙核心，主动帮助并智能地阻止威胁，保护物联网设备，并推荐安全策略。新版本防火墙集合了四大创新功能：基于机器学习技术的本地恶意软件和网络钓鱼防御功能、零延迟签名更新、基于机器学习技术的集成物联网安全，和基于机器学习技术的安全策略。基于机器学习技术的下一代防火墙将在以下四点为企业提高安全运营效率：第一，即时防范高达 95%的未知文件和 Web 威胁；第二，自动提供安全策略建议；第三，提供实时防御功能；第四，扩展可视性和安全性至所有设备，无需部署额外的传感器。

图33：嵌入机器学习技术为防火墙带来性能提升

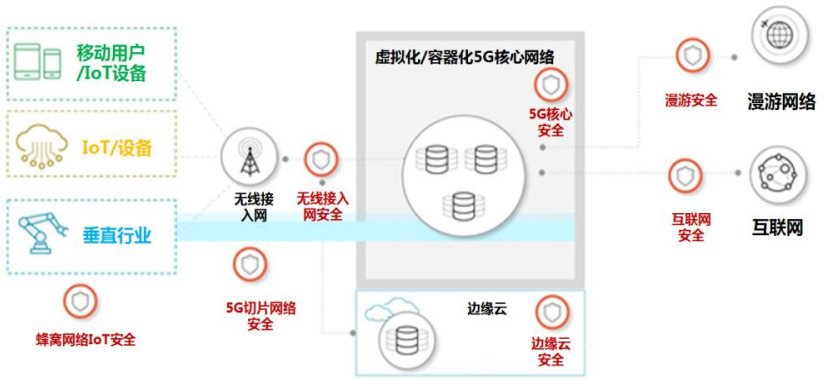


资料来源：SecurityBoulevard

4.2、 推出支持 5G 网络的原生安全产品，紧跟技术变化

公司持续跟随产业技术变化而创新，开发 5G 原生产品。2020 年 11 月 19 日，公司推出业界首款 5G 原生安全产品，帮助服务提供商和企业实现高度安全的 5G 网络环境。该产品将基于下一代防火墙设备部署 5G 安全功能，包括所有 PA 系列、VM 系列、与 CN 系列防火墙产品。5G 原生安全产品将提供三点全新功能：第一，容器化 5G 安全功能；第二，5G 用户或设备威胁的实时可视性、预防与关联；第三，5G 网络切片安全功能。

图34：公司 5G 原生安全产品覆盖全面



资料来源：IT 运维网

5、 投资建议

Palo Alto 作为下一代防火墙的龙头，持续加强在云安全、安全运营等方向的投入，实现向“下一代”安全的成功升级。可以看到，近年来国内安全厂商在完善传统安全产品体系的同时，也在不断加强在云安全、大数据安全、物联网安全领域的布局，积极推进云计算、大数据、人工智能等技术在安全领域的应用。我们认为从传统安全领域向下一代安全领域的延伸及升级成为老牌安全厂商发展必由之路，Palo Alto 的发展路径实际上对我国专业安全厂商非常具有借鉴意义。建议关注网安领域综合实力强，同时在“下一代”安全布局领先的厂商，推荐深信服、奇安信、安恒信息、绿盟科技、启明星辰、美亚柏科，其他受益标的包括天融信、山石网科等。

表6：建议关注网安领域综合实力强，同时在“下一代”安全布局领先的厂商（截至 2021.3.12 收盘）

证券代码	公司简称	当前市值（亿元）	归母净利润（亿元）			PE			PS			
			2020E	2021E	2022E	2020E	2021E	2022E	2020E	2021E	2022E	评级
300454.SZ	深信服	912.20	8.03	10.84	14.6	113.6	84.2	62.5	16.7	11.8	8.8	买入
688023.SH	安恒信息	175.19	1.37	1.91	2.56	127.9	91.7	68.4	13.3	9.4	6.9	买入
688561.SH	奇安信	719.31	-3.29	1.66	6.72	-218.6	433.3	107.0	17.3	12.8	9.7	买入
300369.SZ	绿盟科技	119.16	3.07	4.19	5.58	38.8	28.4	21.4	5.9	4.6	3.6	买入
002439.SZ	启明星辰	294.08	8.54	11.09	14.02	34.4	26.5	21.0	8.0	6.2	5.0	买入
300188.SZ	美亚柏科	141.89	3.76	4.86	6.23	37.7	29.2	22.8	5.9	4.5	3.5	买入

数据来源：Wind、开源证券研究所

6、 风险提示

政府及企业 IT 支出缩减；市场竞争加剧；人才流失风险。

特别声明

《证券期货投资者适当性管理办法》、《证券经营机构投资者适当性管理实施指引（试行）》已于2017年7月1日起正式实施。根据上述规定，开源证券评定此研报的风险等级为R4（中高风险），因此通过公共平台推送的研报其适用的投资者类别仅限定为专业投资者及风险承受能力为C4、C5的普通投资者。若您并非专业投资者及风险承受能力为C4、C5的普通投资者，请取消阅读，请勿收藏、接收或使用本研报中的任何信息。
因此受限于访问权限的设置，若给您造成不便，烦请见谅！感谢您给予的理解与配合。

分析师承诺

负责准备本报告以及撰写本报告的所有研究分析师或工作人员在此保证，本研究报告中关于任何发行商或证券所发表的观点均如实反映分析人员的个人观点。负责准备本报告的分析师获取报酬的评判因素包括研究的质量和准确性、客户的反馈、竞争性因素以及开源证券股份有限公司的整体收益。所有研究分析师或工作人员保证他们报酬的任何一部分不曾与，不与，也将不会与本报告中具体的推荐意见或观点有直接或间接的联系。

股票投资评级说明

	评级	说明
证券评级	买入（Buy）	预计相对强于市场表现 20%以上；
	增持（outperform）	预计相对强于市场表现 5%～20%；
	中性（Neutral）	预计相对市场表现在－5%～＋5%之间波动；
	减持	预计相对弱于市场表现 5%以下。
行业评级	看好（overweight）	预计行业超越整体市场表现；
	中性（Neutral）	预计行业与整体市场表现基本持平；
	看淡	预计行业弱于整体市场表现。
备注：评级标准为以报告日后的 6~12 个月内，证券相对于市场基准指数的涨跌幅表现，其中 A 股基准指数为沪深 300 指数、港股基准指数为恒生指数、新三板基准指数为三板成指（针对协议转让标的）或三板做市指数（针对做市转让标的）、美股基准指数为标普 500 或纳斯达克综合指数。我们在此提醒您，不同证券研究机构采用不同的评级术语及评级标准。我们采用的是相对评级体系，表示投资的相对比重建议；投资者买入或者卖出证券的决定取决于个人的实际情况，比如当前的持仓结构以及其他需要考虑的因素。投资者应阅读整篇报告，以获取比较完整的观点与信息，不应仅仅依靠投资评级来推断结论。		

分析、估值方法的局限性说明

本报告所包含的分析基于各种假设，不同假设可能导致分析结果出现重大不同。本报告采用的各种估值方法及模型均有其局限性，估值结果不保证所涉及证券能够在该价格交易。

法律声明

开源证券股份有限公司是经中国证监会批准设立的证券经营机构，已具备证券投资咨询业务资格。

本报告仅供开源证券股份有限公司（以下简称“本公司”）的机构或个人客户（以下简称“客户”）使用。本公司不会因接收人收到本报告而视其为客户。本报告是发送给开源证券客户的，属于机密材料，只有开源证券客户才能参考或使用，如接收人并非开源证券客户，请及时退回并删除。

本报告是基于本公司认为可靠的已公开信息，但本公司不保证该等信息的准确性或完整性。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金融工具的邀请或向人做出邀请。本报告所载的资料、意见及推测仅反映本公司于发布本报告当日的判断，本报告所指的证券或投资标的的价格、价值及投资收入可能会波动。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。客户应当考虑到本公司可能存在可能影响本报告客观性的利益冲突，不应视本报告为做出投资决策的唯一因素。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。本公司未确保本报告充分考虑到个别客户特殊的投资目标、财务状况或需要。本公司建议客户应考虑本报告的任何意见或建议是否符合其特定状况，以及（若有必要）咨询独立投资顾问。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。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。若本报告的接收人非本公司的客户，应在基于本报告做出任何投资决定或就本报告要求任何解释前咨询独立投资顾问。

本报告可能附带其它网站的地址或超级链接，对于可能涉及的开源证券网站以外的地址或超级链接，开源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分，客户需自行承担浏览这些网站的费用或风险。

开源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。开源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。

开源证券研究所

上海
地址：上海市浦东新区世纪大道1788号陆家嘴金控广场1号楼10层
邮编：200120
邮箱：research@kysec.cn

深圳
地址：深圳市福田区金田路2030号卓越世纪中心1号楼45层
邮编：518000
邮箱：research@kysec.cn

北京
地址：北京市西城区西直门外大街18号金贸大厦C2座16层
邮编：100044
邮箱：research@kysec.cn

西安
地址：西安市高新区锦业路1号都市之门B座5层
邮编：710065
邮箱：research@kysec.cn