2021年中国云抗DDoS服务系列报告（二）：DDoS服务形态与部署现况

2021 China Cloud Anti-DDoS Service Report Series (2): Service Form and Deployment Status

2021年の中国のクラウドアンチDDoS攻撃サービス報告書シリーズ（2）：サービスのフォームと展開状況

报告标签：IPV6、云抗Ddos服务、云安全

头豹研究院简介

- 头豹研究院是中国大陆地区首家**B2B模式人工智能技术的互联网商业咨询平台**，已形成集**行业研究**、**政企咨询**、**产业规划**、**会展会议**行业服务等业务为一体的一站式行业服务体系，整合多方资源，致力于为用户提供最专业、最完整、最省时的行业和企业数据库服务，帮助用户实现知识共建，产权共享
- 公司致力于以优质商业资源共享为基础，利用**大数据**、**区块链**和**人工智能**等技术，围绕**产业焦点**、**热点**问题，基于**丰富案例**和**海量数据**，通过开放合作的研究平台，汇集各界智慧，推动产业健康、有序、可持续发展

300+
资深分析师和研究员

2,500+
细分行业进行深入研究

2万+
注册机构用户
公司目标客户群体覆盖率高，PE/VC、投行覆盖率达80%

25万+
数据元素

50万+
行业专家库

四大核心服务

企业服务

为企业提供**定制化报告**服务、**管理咨询**、**战略**调整等服务

云研究院服务

提供行业分析师**外派驻场**服务，平台数据库、报告库及内部研究团队提供技术支持服务

行业排名、展会宣传

行业峰会策划、**奖项**评选、行业**白皮书**等服务

园区规划、产业规划

地方**产业规划**，**园区**企业孵化服务

报告阅读渠道

- 1、头豹科技创新网 —— www.leadleo.com PC端阅读全行业、千本研报

- 2、头豹小程序 —— 微信小程序搜索“头豹”、手机扫上方二维码阅读研报

- 3、添加右侧头豹研究院分析师微信，邀您进入行研报告分享交流微信群

图说

表说

专家说

数说

扫一扫

实名认证行业专家身份

详情咨询

客服电话

400-072-5588

南京

杨先生： 13120628075

唐先生： 18014813521

上海

王先生： 13611634866

李女士： 13061967127

深圳

李先生： 18916233114

李女士： 18049912451

概览摘要

常规型抗D模块大致驱动，市场价值点在何处？

DDoS攻击(分布式拒绝服务攻击）是指依靠客户与服务器技术将多台计算机（又称“肉鸡”）联合操控以形成规模化的攻击平台，进而对单或多攻击目标发起成倍杀伤力的网络攻击。

抗DDoS服务商在云清洗平台搭建方式与底层应用技术及服务项目细分仍存在差异，但整体常规型DDoS缓解服务的服务模块及其对应计费模式大致驱同；其服务可粗略划分为基础防护、云清洗服务、高防服务、专家运维、防护定制五大模块。

2020年后，网络安全新规相继颁布，中国网络安全保护进入新阶段，带动企业网络安全意识强化，未来抗DDoS等安全行业发展具备增长性与确定性。

01 常规型云抗D服务与计费模式大致趋同

虽然各服务商在云清洗平台搭建方式与底层应用技术及服务项目细分仍存在差异，但整体常规型DDoS缓解服务的服务模块及其对应计费模式大致驱同；其服务可粗略划分为基础防护、云清洗服务、高防服务、专家运维、防护定制五大模块。

02 DDoS防护等安全行业发展具备增长性与确定性

2020年中国DDoS防护在下游客户接受度上存在大量上升空间，仍有部分企业对DDoS攻击存在逃避心理。但2021年后，《关键信息基础设施安全保护条例》等网络安全新规相继颁布，中国网络安全保护进入新阶段，带动企业网络安全意识强化，未来预计DDoS防护等安全行业发展具备增长性与确定性。

03 产业成熟度及下游客户接受度预计将双向提升

安全即服务模式下，产业成熟度及下游客户接受度预计将双向提升，有望带动云抗DDoS服务逐步成为抗DDoS安全行业的核心增量来源。硬件市场方面，替代趋势下，短期承压，但整体市场细分场景下安全敏感度及应用需求的差异，传统硬件市场存量份额较为稳固

目录

Contents

名词解释

- **DDoS：**denial-of-service attack，一种网络攻击手法，其目的在于使目标电脑的网络或系统资源耗尽，使服务暂时中断或停止，导致其正常用户无法访问。
- **IPV4：**Internet Protocol version 4，一种无连接的协议，操作在使用分组交换的链路层（如以太网）上。此协议会尽最大努力交付数据包，意即它不保证任何数据包均能送达目的地，也不保证所有数据包均按照正确的顺序无重复地到达。这些方面是由上层的传输协议（如传输控制协议）处理的。
- **IPV6：**Internet Protocol version 6，网际协议的最新版本，用作互联网的协议。用它来取代IPv4主要是为了解决IPv4地址枯竭问题，同时它也在其他方面对于IPv4有许多改进。
- **骨干网：**计算机网络的一部分，它将各个网络相互连接起来，使得不同的局域网或子网之间能进行信息交换[1]。骨干网可以将同一建筑物内、校园环境中不同建筑物内或广大区域内的不同网络连接在一起。通常情况下，骨干网的容量要大于与其相连的网络容量。
- **肉鸡：**接入互联网受恶意软件感染后，受控于黑客的电脑。其可以随时按照黑客的命令与控制（C&C, command and control）指令展开拒绝服务（DoS）攻击或发送垃圾信息。通常，一部被侵占的电脑只是僵尸网络里面众多中的一个，会被用来去运行一连串的或远程控制的恶意程序。
- **物联网：**计算设备、机械、数字机器相互关系的系统，具备通用唯一识别码（UID），并具有通过网络传输数据的能力，无需人与人、或是人与设备的交互。

Chapter 1
服务形态分析

- 基础服务模块满足云上资产日常防护需求，增加产品使用粘性，巩固产品生态。同时透过生态客群反向为云抗D服务引流
- 云清洗服务通过基于规则和人工智能算法快速识别源站流量，将攻击流量分流牵引至清洗中心，进而将安全流量回注源站服务器
- 高防服务模块通过将用户域名解析至高防IP，定向公网流量流经高防IP集群，应用端口协议转发将安全流量转发至源站
- 抗DDoS一线防护团队、防护经验丰富，可快速识别攻击类型，针对不同业务场景及攻击模式提供对应防护预案

云抗DDoS服务形态分析——服务形态总览

- 常规型云抗D服务划分为基础防护、云清洗服务、高防服务、专家运维、防护定制五大模块

云抗DDoS服务形态

常规型云抗DDoS服务模块

防护模块	防护核心	防护效用	防护场景
1 基础防护	实时监测 基础防护	■ *为确保云上产品运行稳定，云平台厂商提供免费实时流量监测及基础流量防护服务* ■ *无需安装与运维。* ■ *但防护攻击种类较单一，可抵御流量通常在5GB以下，防护能力较弱*	■ *偏向于客户需求刚性、攻击频率及攻击流量相对较低的中小企业防护场景*
2 云清洗服务	快速识别 流量清洗	■ *有效识别攻击流量* ■ *通过DNS或BGP牵引将攻击流量牵引至清洗中心或高防数据中心，进而将清洗流量回注源站* ■ *可抵御150G以上流量攻击*	■ *云清洗应用较为广泛，场景范围主要以防护价效比及弹性防护诉求高的企用场景*
3 高防服务	高防秒解 业务稳定	■ *使用高防IP配置转发规则及源站回流，或将服务器托管于高防秒解机房，* ■ *有效抵抗大规模流量DDoS攻击* ■ *秒解受攻击IP，最大限度保障源站业务安全稳定。*	■ *主要面向攻击风险高、业务稳定诉求高、用户需求弹性、侧重用户体验的游戏、金融等企业场景*
4 专家运维	人机协同 急时响应	■ *原厂安全团队实战经验丰富，人机协同快速识别攻击类型，急时响应攻击。* ■ *团队技术专业性及数据调用能力占优，并可根据业务特性及攻击场景* ■ *提供灵活防护，大幅缩减DDoS攻击手法、时间、周期不确定性下的高风险*	■ *主要偏向于中大型企业企用场景为主* ■ *其客群具备相应的专家运维、安全策略定制、内部架构调整诉求。* ■ *整体支付能力及支付意愿相对较高，项目利润较可观*
5 防护定制	架构调整 策略定制	■ *根据客户资产环境及防护诉求，制定综合完整防护方案，* ■ *安全策略定制、架构调整、运维部署、防护前置等，以巩固完善企业抗D防护体系*	

防护成本

Akamai、头豹研究院

- **DDoS攻击属于技术无解问题，云抗D服务形态并非固定，需根据应用客户垂直行业的差异化诉求及攻击场景灵活组合抵御和缓解**

DDoS核心攻击思路是利用协议特性和系统弱点消耗其系统资源，进而重点打击目标源站网络安全可用性，属于技术无解问题。同时，由于DDoS攻击的攻击手法多变、突发性强，整体抗D防护更偏向于完整的系统性工程，涉及安全服务、专家运维、方案定制、威胁情报等多维安全防护，难以依赖标准化方案和单一服务抵御和缓解。因此，云抗D服务形态并非固定，需根据应用客户垂直行业的差异化诉求及攻击场景灵活组合。

- **常规型云抗D服务划分为基础防护、云清洗服务、高防服务、专家运维、防护定制五大模块**

由于云抗DDoS市场厂商较为多元，其带宽资源、技术防护、服务生态、节点分布等多维度均存在较大差异，因此市场中云抗DDoS防护手段及服务类型较为多元。其中，以网络运营商最为特殊。不同于常于其他厂商，网络运营商DDoS缓解服务主要针对于百G规模以上的大流量的协议层清洗和流量压制，而非针对应用层。该类服务商带宽富用程度远高于其他服务商，同时可调用核心网路由器数据对经过营运商网络的任意互联网目标IP进行在线实时流量监控，监控覆盖面广，大流量规模测度准确性高，攻击溯源能力占优。但营运商云DDoS缓解仅能实现单线BGP。若涉及跨营运商攻击流量清洗，可用带宽相对较小。此外，其数据检测基于Netflow抽样，以慢速攻击代表的低流量攻击的检测效果较差。

云抗DDoS服务形态分析

云抗DDoS服务模块效益与价格

扫码查看高清图片

https://www.leadleo.com/ill/details?id=6132034031d32d6c26da730c&core=6143cc7e0dd1776ba95604d5

Akamai、头豹研究院

整体来看，营运商市场化程度较低，尚无成熟的价格体系；标的客群主要集中于大型互联网公司、IDC、二级SP及其大型央国企专线网络客户等，整体客群门槛相对较高。而就其他厂商而言，虽然各服务商在云清洗平台搭建方式与底层应用技术及服务项目细分仍存在差异，但整体常规型DDoS缓解服务的服务模块及其对应计费模式大致驱同；其服务可粗略划分为基础防护、云清洗服务、高防服务、专家运维、防护定制五大模块。

云抗DDoS服务形态分析分析——基础服务模块

- 基础服务模块满足云上资产的日常防护需求，增加产品使用粘性，巩固产品生态。同时，透过生态客群及免费模式反向为云抗D服务引流

扫码查看高清图片

https://www.leadleo.com/ill/details?id=6132036431d32d6c26da7311&core=6143cc820dd1772403560539

安全即服务（周凯）、CSDN、头豹研究院

- **基础防护是云抗DDoS初级形式，透过云产品生态客群及免费模式反向为云抗D服务引流，培养基础的客户需求**

纵观常规型云抗DDoS产品，基础防护是云抗DDoS初级形式，其核心效用在于为针对云服务器等云上资产提供基础且日常的抗D防护及攻击流量统计。

该服务模块通常由云平台服务商提供，主打免费、无安装、无运维、自发防护，一方面通过利用冗余带宽资源相应满足普通用户云上资产的日常防护及业务稳定需求，增加该云产品使用粘性，巩固其产品生态。另一方面，透过产品生态客群及免费模式反向为云抗D服务引流，培养基础的客户需求，进一步挖掘潜在客群。

- **基础防护攻击种类较单一，防护能力较弱，主要应用于业务稳定敏感度相对较低或攻击频率较小的中小企业场景**

但在防护能力方面，基础防护攻击种类较单一，仅可抵御5GB以下攻击流量。若攻击流量超过该阈值，系统将对超过黑洞阈值的受攻击公网IP进行黑洞处理，导致受攻击源站正常访问流量丢弃，客户业务不可用。因此，基础防护现主要应用于业务稳定敏感度相对较低或攻击频率较小的中小企业场景。

云抗DDoS服务形态分析——云清洗模块

- **云清洗服务通过基于规则和人工智能算法快速识别源站流量，将攻击流量分流牵引至清洗中心，进而将清洗后安全流量回注源站服务器**

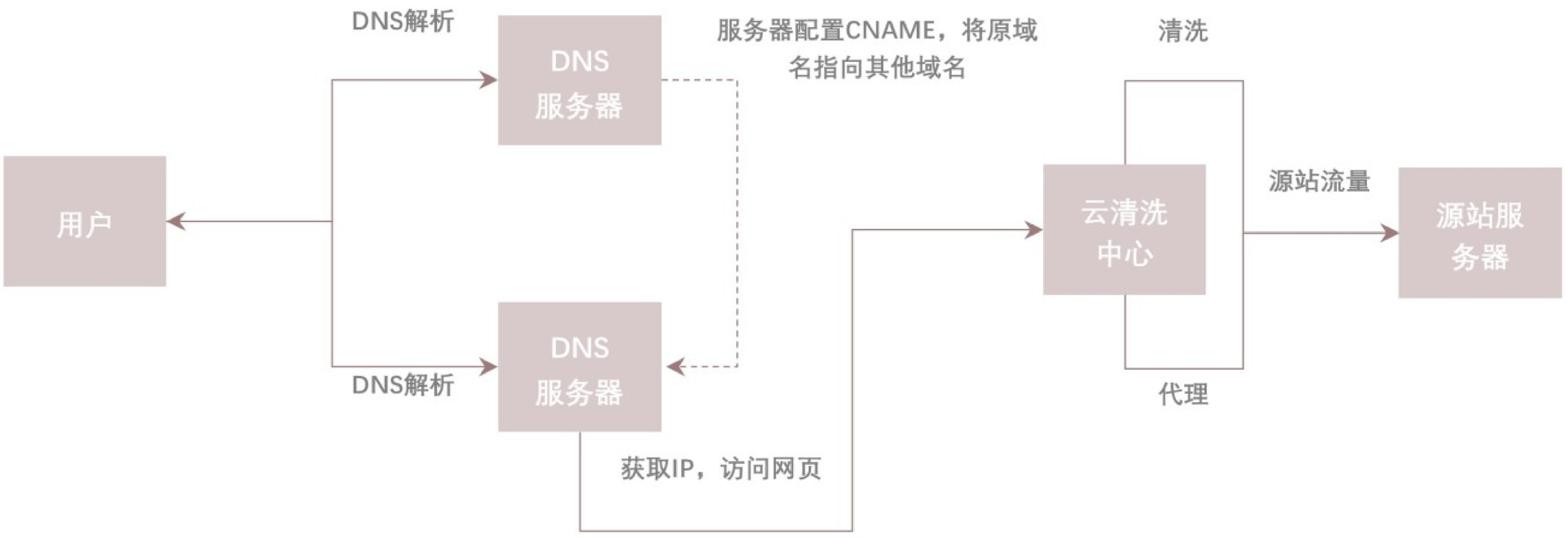
- **清洗服务模块做为云抗D服务的基础形态，防御攻击类型及防护流量方面优势显著，也是抗D客群优先选择的方式之一**

相较之下，云清洗服务模块做为云抗D服务的基础形态，防御攻击类型及防护流量方面优势显著，也是抗D客群优先选择的方式之一。云清洗服务可通过基于规则和人工智能算法快速识别源站用户流量与攻击流量，并将攻击流量分流牵引至清洗中心，进而将清洗后安全流量回注源站服务器，可有效抵御150GB以上的攻击流量。根据流量牵引的工作机制分类，云清洗服务模块主要划分为DNS牵引与BDP牵引两种：

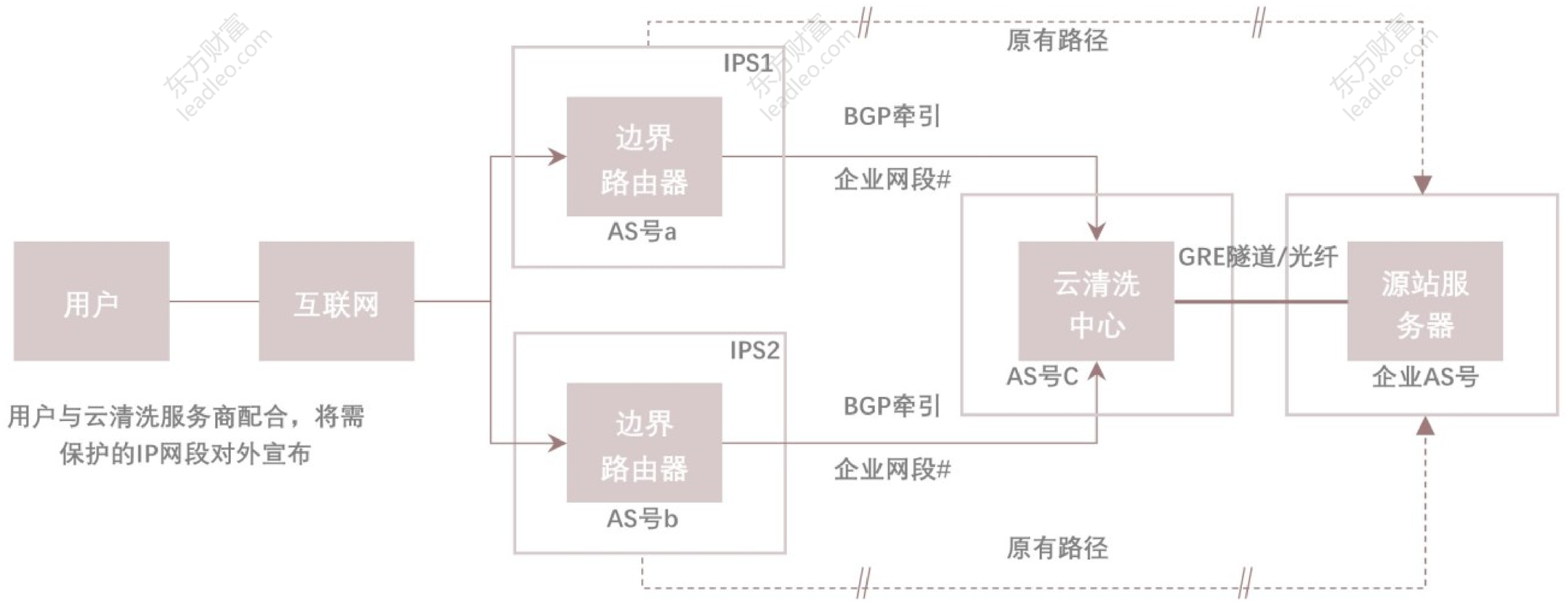
安全即服务（周凯）、CSDN、头豹研究院

云清洗模块

DNS牵引模式工作机制



BGP模式工作机制



DNS牵引模式

a) 从用户侧的角度分析，DNS牵引配置方式较为简便，仅需更改DNS配置便可对单个网站进行防护。同时，DNS牵引模式整体结构清晰，架构内的云清洗中心效用可相当于CDN代理服务器：同步实现流量清洗与转发，大幅缓解DDoS攻击，同时隐藏源服务器IP地址，进一步巩固抗D防护体系。但DNS模式引发一定程度的时间延迟，较不适应与业务稳定度及清洗速度要求较高的应用场景。此外，该牵引模式需同时采取IP访问控制及更换IP措施，以避免源站IP地址暴露引发的攻击绕过行为。

安全即服务（周凯）、CSDN、头豹研究院

BGP牵引模式

a) 不同于DNS模式针对单一网站及IP地址的牵引，BGP牵引形模式无需针对不同协议或特定代理服务器，可对覆盖全网络段的流量进行牵引定向，并有效保护企业内网资源，应用于中大企业场景中。但BGP配置相对较为复杂，需专业网络安全运维人员对两侧环境进行配置调试。BGP收敛时间相对较为长。

在收费模式方面，云清洗服务模块是基于弹性付费，用户可根据在某一时期内所需DDoS流量防护峰值、CC防护能力、回源带宽等定制服务，整体客户企业投入其与需求更贴近、匹配度更高。

但当攻击流量超过阈值时，系统仍将进行黑洞处理，避免攻击持续影响全部客户的稳定性。因此，依靠单一云清洗服务模块仍然难以绝对保障客户7*24小时的业务稳定，安全防护仍存在风险。

云抗DDoS服务形态分析——高防服务模块

- **高防服务模块通过将用户域名解析至高防IP，定向公网流量流经高防IP集群，应用端口协议转发将清洗过滤后的安全流量转发至源站**

❑ **高防服务模块是云抗DDoS服务增值服务模块，通过将用户域名解析至高防IP并同时设置转发规则确保源站的安全稳定**

高防服务模块是云抗DDoS服务增值服务模块，其主要通过将用户域名解析至高防IP并同时设置转发规则，定向公网流量流经高防IP集群。同时，应用端口协议转发将清洗过滤后的安全流量转发至源站，进而透过复用流量确保源站的安全稳定。

从用户侧的角度看，高防服务核心优势有二：

无需数据迁移、操作简便

1) 无需数据迁移与提前部署，用户仅需在遭遇攻击时更改设置，操作便捷。

安全即服务（周凯）、CSDN、头豹研究院

弹性扩容、攻击秒解

1) 由于高防IP服务基于集群架构，其抗DDoS防护具备弹性扩容能力。用户可有效跟进攻防对抗趋势，秒解受攻击IP，并同时有效隐藏站源IP、保证业务的稳定运行，整体DDoS防护性价比较高。针对上述服务特性，高防服务主要应用于在线游戏、金融、电商等业务稳定敏感度及用户体验实时性要求高的高价值云抗DDoS场景。但短期来看，高防IP服务模块整体误杀率相对较高。当用户启用严格防护模式时，高防IP服务将屏蔽掉部分公用IP及Wi-fi。同时，高防IP服务仅是基于转发规则，其运行速度与服务器保持正比，并不具备加速效用。

云抗DDoS服务形态分析——专家运维与防护定制模块

- **云抗D服务商提供一线防护团队，抗DDoS防护经验丰富，可快速识别攻击类型，针对不同业务场景及攻击模式提供对应防护预案**

❑ **抗DDoS攻防之间具备滞后性，企业安全策略需实时调整，平衡把控业务存活及安全防护，对后端运维人员专业性、响应及时性要求较高**

整体来看，随着DDoS攻击方式日趋多元化、复杂化，不同攻击手段将随着攻击场景、攻击技术、防护态势等因素而改变，难以依赖标准化云抗DDoS服务预案。

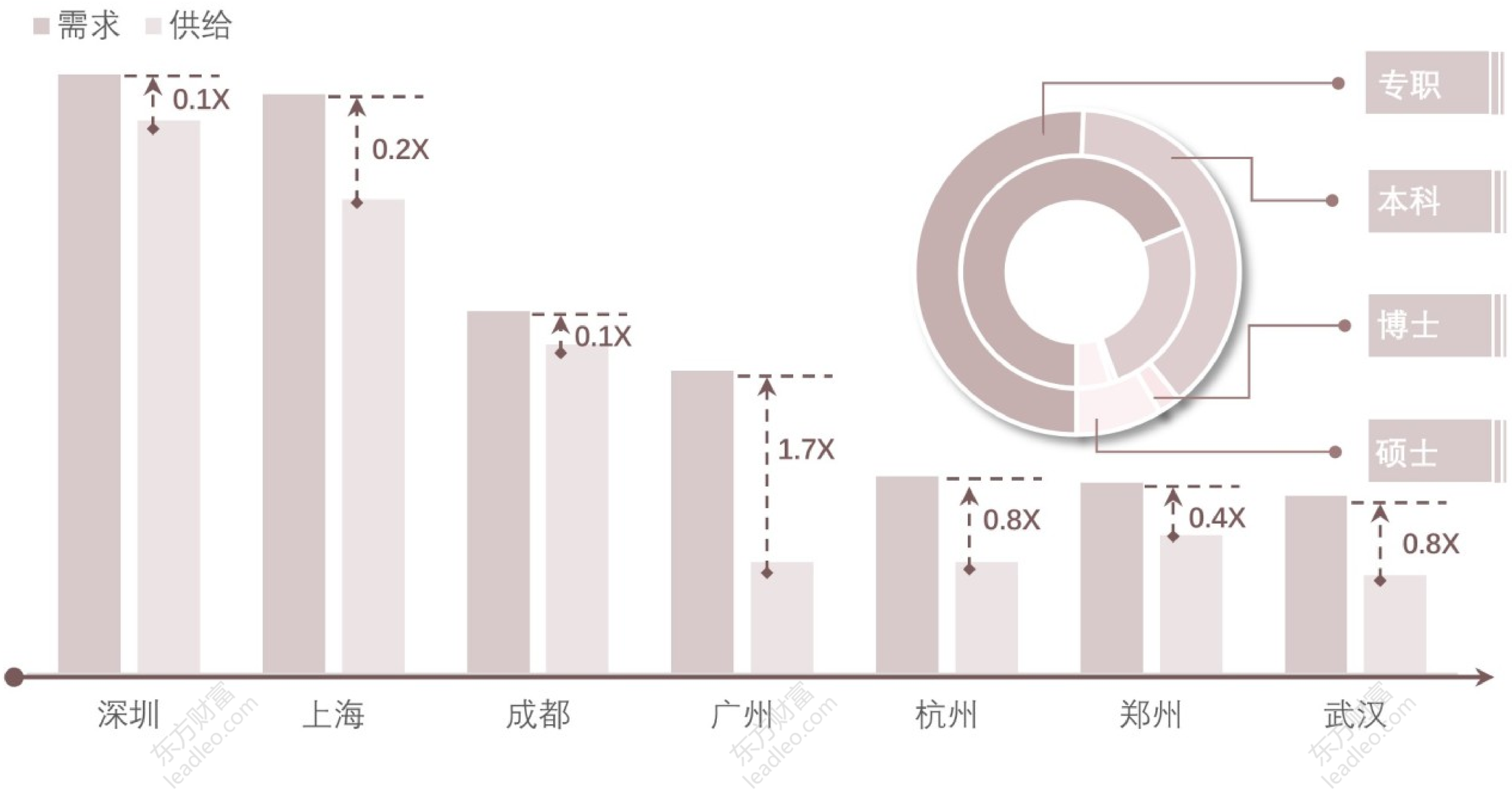
同时，由于抗DDoS攻防之间具备滞后性，企业安全策略需实时调整，平衡把控业务存活及安全防护，对后端安全运维人员专业性、响应及时性要求较高。然后，2019年起，中国市场安全从业人员较为紧缺，人才短板问题日益加重。根据头豹数据显示，相较于2019年，中国网络安全人才需求量同比上涨250%。其中，深圳、上海、成都等多主要城市出现网络安全人才短缺现象严重。对于常规型企业而言，安全人才培养难度较大、时间及财务成本高，因而阻碍其实时调整安全战略，造成其安全防护缺口。

而专家运维服务模块可动用云抗D服务商内部的一线防护团（承接上文）

安全即服务（周凯）、CSDN、头豹研究院

专业运维人员需求缺口

网络安全人才供需情况与学历职位供需分布差异



（承接下文）队，抗DDoS防护经验丰富，可快速识别攻击类型，针对不同业务场景及攻击模式提供对应防护预案，大幅提升企业安全体系防护能力。以CC攻击为例，不同于大流量攻击，CC攻击主要依赖信息查询与信息修改等高频请求绕过前端业务，对后端业务数据库实施长效连锁打击效果。针对该类攻击，需动用人工处理将被攻击的业务点拉黑，进而实现小规模攻击点的快速拦截。此外，专家运维模块可对互联网攻击事件实时监控，第一时间获取最新攻击手段及攻击数据，急时研究对应处理预案，进而大幅缩减攻击防护难度及团队攻击响应周期。该类服务模块通常应用于中层以上云抗DDoS产品。

- **定制化防护方案涵盖安全策略定制、架构调整、运维部署定制等子服务项，偏向于支付能力及支付意愿相对较高的中大企业级政府场景**

云抗DDoS服务商也可为企业客户提供定制化的安全防护方案。该服务模块涵盖安全策略定制、架构调整、运维部署定制等子服务项，针对客户业务、资产环境、应用场景等因素提供全面的防护方案，进而完善客户抗DDoS安全体系，减少木桶效应风险。然后，专家运维服务模块及方案定制模块的服务价格相对较高，现主要偏向于支付能力及支付意愿相对较高的中大企业级政府场景

安全即服务（周凯）、CSDN、头豹研究院

Chapter 2
产品现况分析

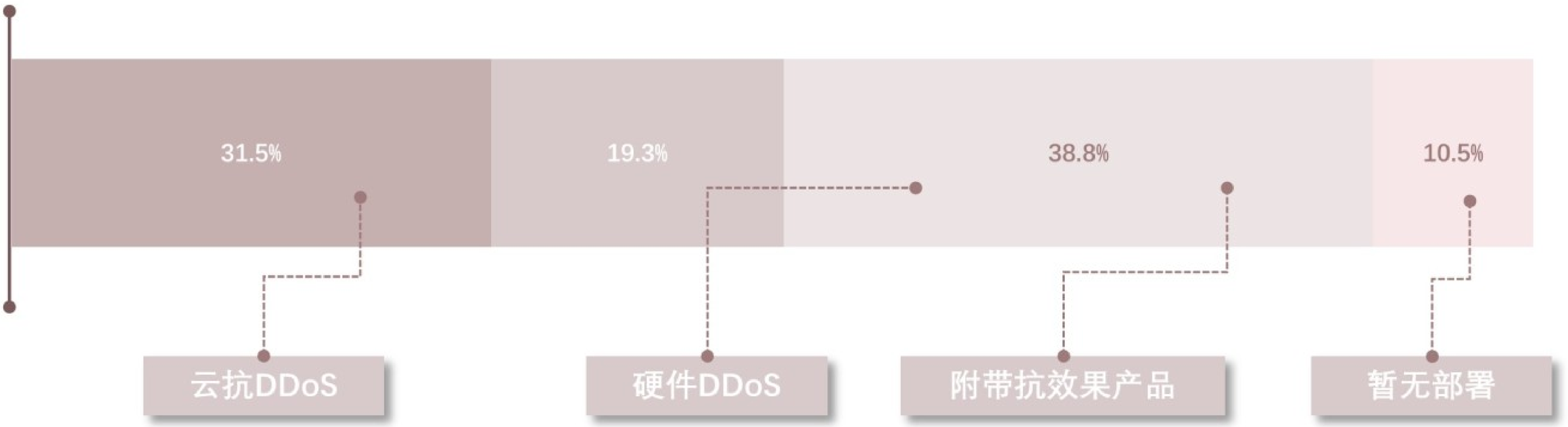
- 网络安全新规相继颁布，中国网络安全保护进入新阶段，带动企业网络安全意识强化，未来抗DDoS等安全行业发展具备增长性与确定性
- 相较于硬件抗DDoS本地部署，云端部署DDoS凭借服务优势、弹性收费、客群生态等优势逐步形成市场替代
- 替代趋势下，硬件市场短期承压，但整体市场细分场景下安全敏感度及应用需求的差异，传统硬件市场存量份额较为稳固
- CC防护、攻击溯源、攻击信息可视化是市场最为重点关注及期待提升的三种能力，未来有望成为抗DDoS市场价值亮点

云抗DDoS产品现况分析——抗DDoS部署现况

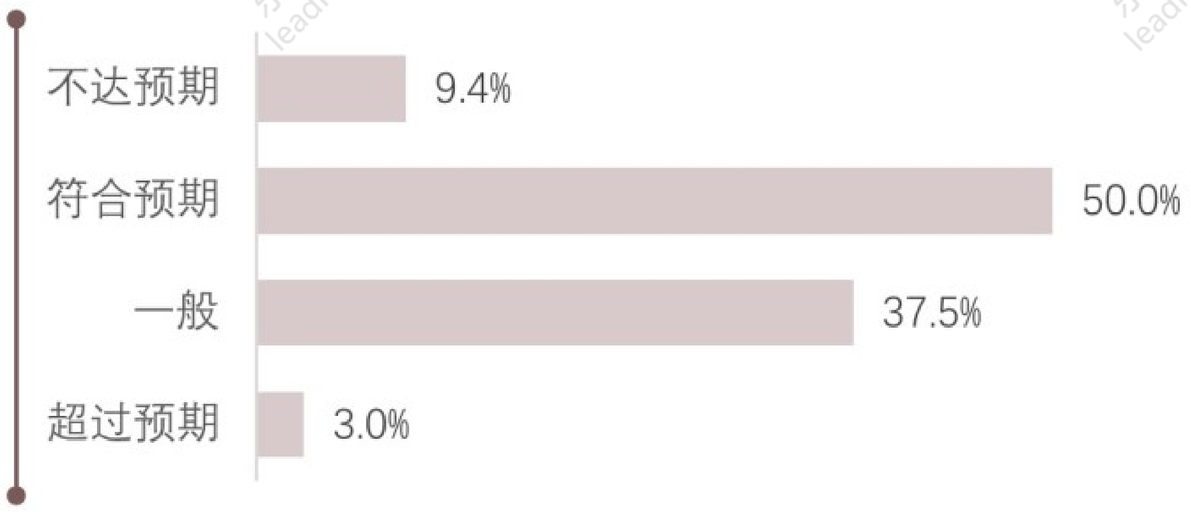
- 针对抗DDoS防护需求，专业抗D产品仍是市场首选；下游客户接受度上存在大量上升空间，仍有部分企业对DDoS攻击存在逃避心理

抗DDoS部署市场调研结果反馈，2020年

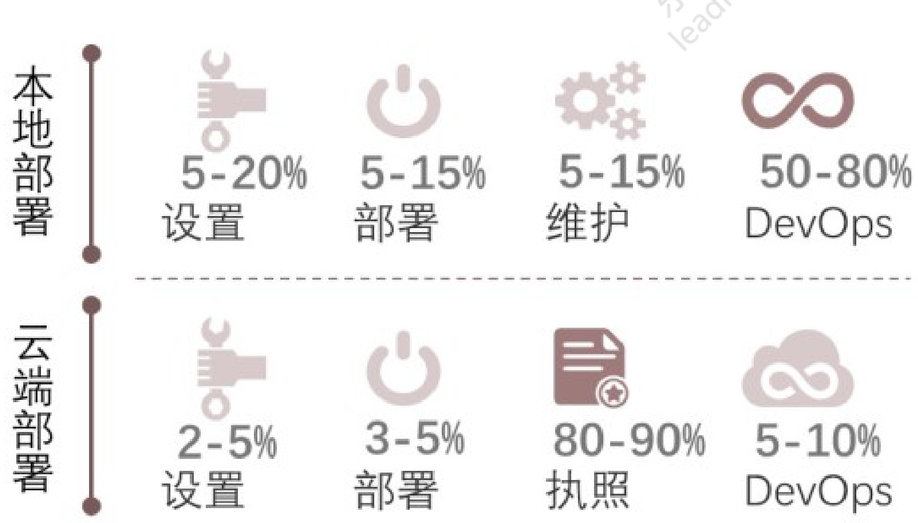
抗DDoS产品使用与部署现况，2020年



抗D产品预期反馈，2020年



云抗D与硬件抗D开销占比，2020年



- **针对抗DDoS防护需求，专业抗D产品仍是市场首选；网络安全新规相继颁布，中国网络安全保护进入新阶段，带动企业网络安全意识强化，未来抗DDoS等安全行业发展具备增长性与确定性**

从市场抗DDoS服务与产品整体的部署情况看，针对抗DDoS防护需求，专业性的云抗DDoS服务及硬件抗DDoS产品凭借其抗D技术及算法的相对优势仍是市场客户的首选。2020年，超过50%以上收调研企业已部署DDoS产品与服务。

然而，仍有48%的受调研企业表示暂无部署意向及仅适用具备抗DDoS能力的网络安全产品，如WAF、IPS等。根据调研结果综合推断（承接上文）

网宿科技，FreeBuf、头豹研究院编辑整理

（承接下文），2020年中国DDoS防护在下游客户接受度上存在大量上升空间，仍有部分企业对DDoS攻击存在逃避心理。

但2021年后，《关键信息基础设施安全保护条例》等网络安全新规相继颁布，中国网络安全保护进入新阶段，带动企业网络安全意识强化，未来预计DDoS防护等安全行业发展具备增长性与确定性。

云抗DDoS产品现况分析——专业抗D产品VS增值抗D产品

- 类附带抗D增值效果的安全产品仅抵御小规规模的应用层DDoS攻击，可作为整体防御策略的一部分，但难以替代专业抗D产品的核心作用

❑ 相较于专业抗DDoS，WAF及IPS等安全产品仅能够抵御小规模的应用层DDoS

根据本次调研的结果显示，市场中仍有38.5%受调研企业选择依赖附带抗DDoS效果的防火墙、IPS、IDS等综合型安全产品进行DDoS攻击的缓解。但整体来看，该类附带抗DDoS增值效果的安全产品仅抵御小规模的应用层DDoS攻击，整体抗DDoS防护能力较为弱势。

以防火墙为例，虽然防火墙是现今最为广泛的网络安全产品之一，但防火墙的设计旨在于实现内部网络与公众访问网（如Internet）的隔离，而非考虑专业的DDoS防护。其抗DDoS的脆弱点主要表现为三方面：

防火墙检测能力限制

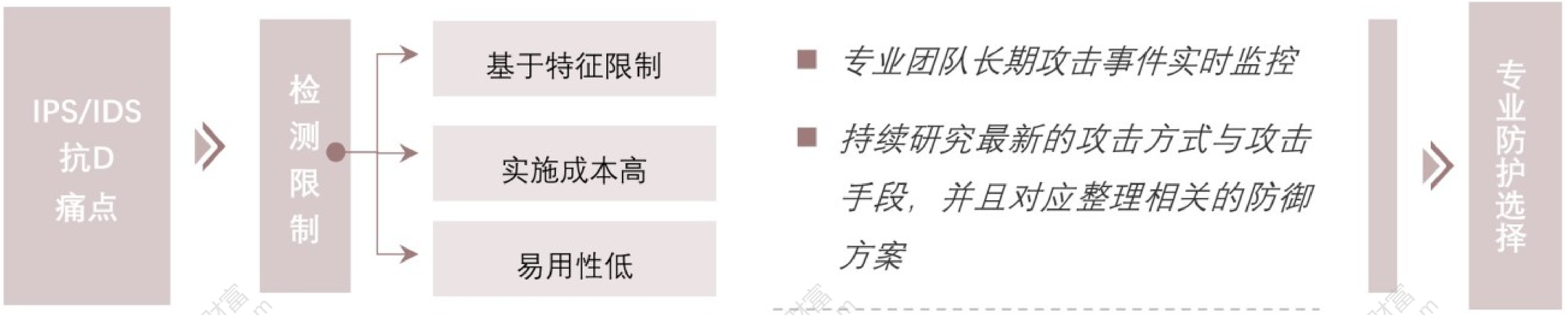
1. 常规部署下，防火墙是作为三层分组转发设备部署与于网络中，可同时实现对内部网络的保护及内外Internet服务通路供应。但在某些应用场景下，若DDoS攻击采用的协议为服务器允许的合法协议，防火墙便无法精确区分正常业务流量与攻击流量，进而造成防御缺口。现阶段而言部分，虽然部分防火墙产品以内置攻击流量检测模块，但该类模块主要基于规则算法为主，而非行为算法。防火墙规则算法属于静态防护操作，难以抵御千变万化的攻击手法。

中国移动通讯，FreeBuf、头豹研究院编辑整理

专业抗DDoS和增值抗DDoS产品对比分析

防火墙 VS 专业抗D

IPS/IDS VS 专业抗D



防火墙算力限制

2. 其次，在算力应用方面，传统额防火墙计算能力存在相应的限制。高强度的流量检测势必会将耗费防火墙额外算力。当DDoS攻击流量规模超过阈值时，防火墙性能将急剧下降，进而难以完成其基本分组转发任务。

中国移动通讯，FreeBuf、头豹研究院编辑整理

防火墙部署弱点

3. 防火墙的部署位置通常设置于网络入口处，其目的在于保护网络内部的所有资源与资产。然而，该部署形式也将成为DDoS攻击标的：攻击者可通过大规模攻击直接招致网络性能大幅下降，进而引发常规用户的访问需求被系统拒绝。

简而言之，防火墙效用更偏向于网络安全员，可助于抗DDoS检测，作为整体防御策略的一部分，而非单一的防护方案。

此外，IPS/IDS同为广泛应用的网络安全检测与防护产品，但其入侵检测仍是基于规则算法，需对协议会话进行还原。但现今DDoS攻击主要采用合法数据分组的攻击流量，这将导致IPS及IDS系统难以对该类型流量进行基于特征的有效检测。

现阶段而言，虽然部分IPS及IDS产品已内置协议异常检测的能力，但仍然需要依赖安全团队的手动配置与运维。相较于专业抗DDoS产品与服务，IPS与IDS的产品易用性及综合抗D能力相对较弱。

云抗DDoS产品现况分析——硬件抗D产品vs云抗D服务

- **相较于硬件抗DDoS本地部署，云端部署DDoS凭借服务优势、弹性收费、客群生态等优势逐步形成市场替代**

❑ **相较于硬件抗Ddo本地部署，云端部署DDoS凭借服务优势、弹性收费、客群生态等优势逐步形成市场替代**

根据市场调研数据显示，在部署DDoS产品与服务企业样本中，选择云端部署DDoS产品的企业占比超过60%以上，较为2019年涨幅约3%，整体云化部署替代趋势较为显著。

其核心原因在于2016年后中国互联网新基建规模日趋庞大，DDoS攻击可用带宽随之增长，传统硬件抗DDoS部署及运维的痛点逐步暴露，主要表现为以下几方面：

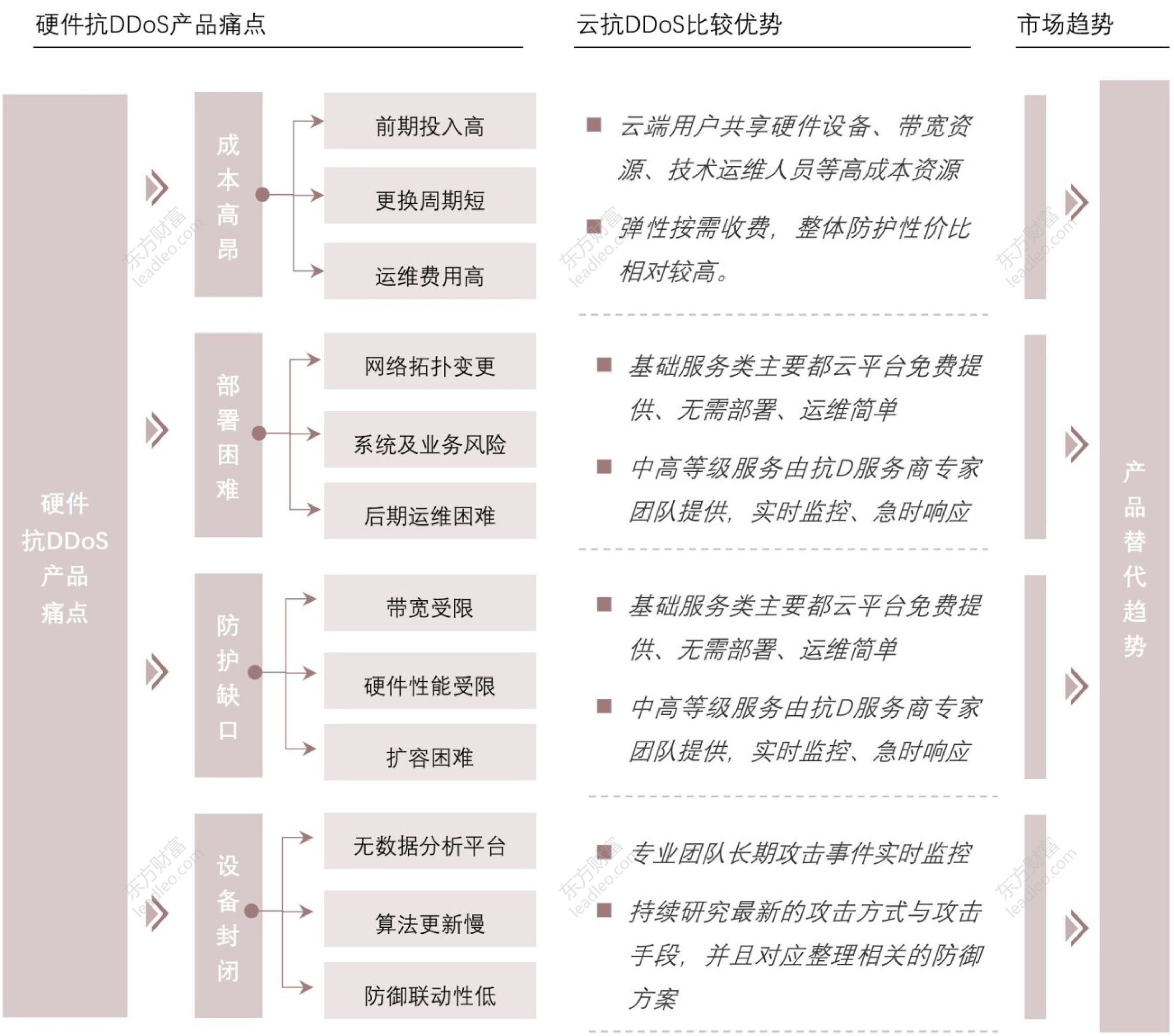
中国移动通讯，FreeBuf、头豹研究院编辑整理

综合抗DDoS防护成本高昂

1. 相较于云端部署抗DDoS产品的弹性收费模式，硬件抗DDoS产品一期前期采购费用在6万至40万不等，平均折旧周期在3-5年，前期投入费用高昂。同时，在变动成本方面，本地化硬件部署需要企业自建安全团队运维进行设备监控、策略调整和升级维护，整体运维投入费用占比更高达（承接上文）

硬件Ddos产品与云抗DDoS服务对比分析

硬件抗DDoS VS 云抗DDoS



中国移动通讯，FreeBuf、头豹研究院编辑整理

1. (承接下文）整体费用的50%至80%以上，进一步缩减其价效比。排除金融等私有云部署场景外，以云清洗为代表的云抗DDoS服务主要基于公有云部署，云端用户可共享硬件设备、带宽资源、技术运维人员等高成本资源，同时弹性按需收费，整体防护性价比相对较高。

部署复杂、防护存在突破点

2. 虽然在互联网接入位置部署串联或旁路部署硬件抗DDoS产品可有效抵御一定规模的DDoS攻击。但串联与旁路部署的方式需对源站网络拓扑变更调整。整体部署流程较为复杂，存在相应的系统及业务风险，后期IT团队运维难度相对较大。此外，当攻击流量高于企业带宽阈值时，硬件抗DDoS防护能力将瞬间失效，将造成企业安全脆弱点，进而引发整体防护体系的木桶效用。

设备数据封闭性强

3. 传统抗DDoS硬件设备封闭性较强，无法形成数据分析平台，整体防御算法更新较慢，难以形成持续且联动防御机制。而云抗DDoS服务则可提供专业团队对全球网络中DDoS攻击事件长期实时监控，持续研究网络中最新的攻击方式与攻击手段，并对应整理相关的防御方案，进而缩减在攻击突发时的应急响应与快速处置周期。

云抗DDoS产品现况分析——抗DDoS产品与服务市场展望

- **安全即服务模式下，产业成熟度及下游客户接受度预计将双向提升，有望带动云抗DDoS服务逐步成为抗DDoS安全行业的核心增量来源**

❑ **相较于硬件抗Ddo本地部署，云端部署DDoS凭借服务优势、弹性收费、客群生态等优势逐步形成市场替代**

以云清洗、高防服务为代表的云抗DDos服务则凭借其服务优势、弹性收费、客群生态等优势在游戏、电商、传媒等等DDoS攻击较集中高、具备较强业务连续稳定性诉求的大型互联网企业场景快速渗透，（承接上文）

中国移动通讯，FreeBuf、头豹研究院编辑整理

（承接下文）逐步相应的替代优势。根据头豹数据显示，2020年大型互联网及游戏、在线金融等场景的云抗DDoS市场份额比已超过过78%。

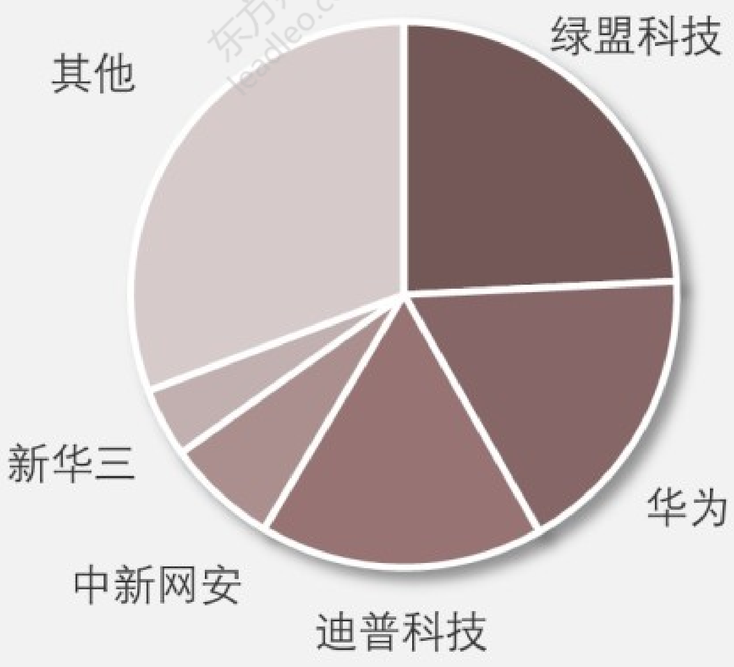
从长期发展的维度看，随着未来中国企业数字化转型进程的演进及云计算应用将持续拓宽，整体安全即服务模式下的产业成熟度及下游客户接受度预计将双向提升，有望带动云抗DDoS服务逐步成为抗DDoS安全行业的核心增量来源。

- **替代趋势下，硬件市场短期承压，但整体市场细分场景下安全敏感度及应用需求的差异，传统硬件市场存量份额较为稳固**

而就中短期而言，虽然替代趋势下，整体硬件抗DDoS市场承压，但鉴于细分行业下安全敏感度及应用需求的差异性，传统硬件抗D产品市场下游需求及市场存量份额较为稳固，未来有望呈现有幅增长态势。在标的客群方面。硬件抗DDoS核心标的客群以运营商及IDC客户为主，年均采购份额占比超85%，整体支付能力及支付意愿均处高位，盈利空间较为可观。但从供应侧的维度看，整体行业偏向于技术密集型。前期硬件研发投入相对较高，同时需要专业运维团队对下游客户提供软硬件长期运维及售后服务，增加用户使用粘性，进而实现对价值客群的长期绑定与铺陈。但DDoS团队整体专业抗D技术实力及攻防经验要求远高于普通安全运维团队及MSS团队，整体团队建设及理论实践的年均投入成本高、周期长。

硬件竞争格局

硬件抗D市场份额，2020年



整体来看，硬件抗D的行业准入门槛相对较高，业内核心玩家相对较小，暂呈现一超多强态势。其中，绿盟科技凭借其优势的智能防护算法、威胁情报资源、技术骨干级攻防团队稳居行业首位。2020年，中国绿盟科技硬件抗DDoS产品市场份额占比超过23%。未来，绿盟有望通过企业集群化硬件大规模部署，结合CDN技术形成云地混合部署抗D综合解决方案，逐步转型渗透云抗DDoS领域。

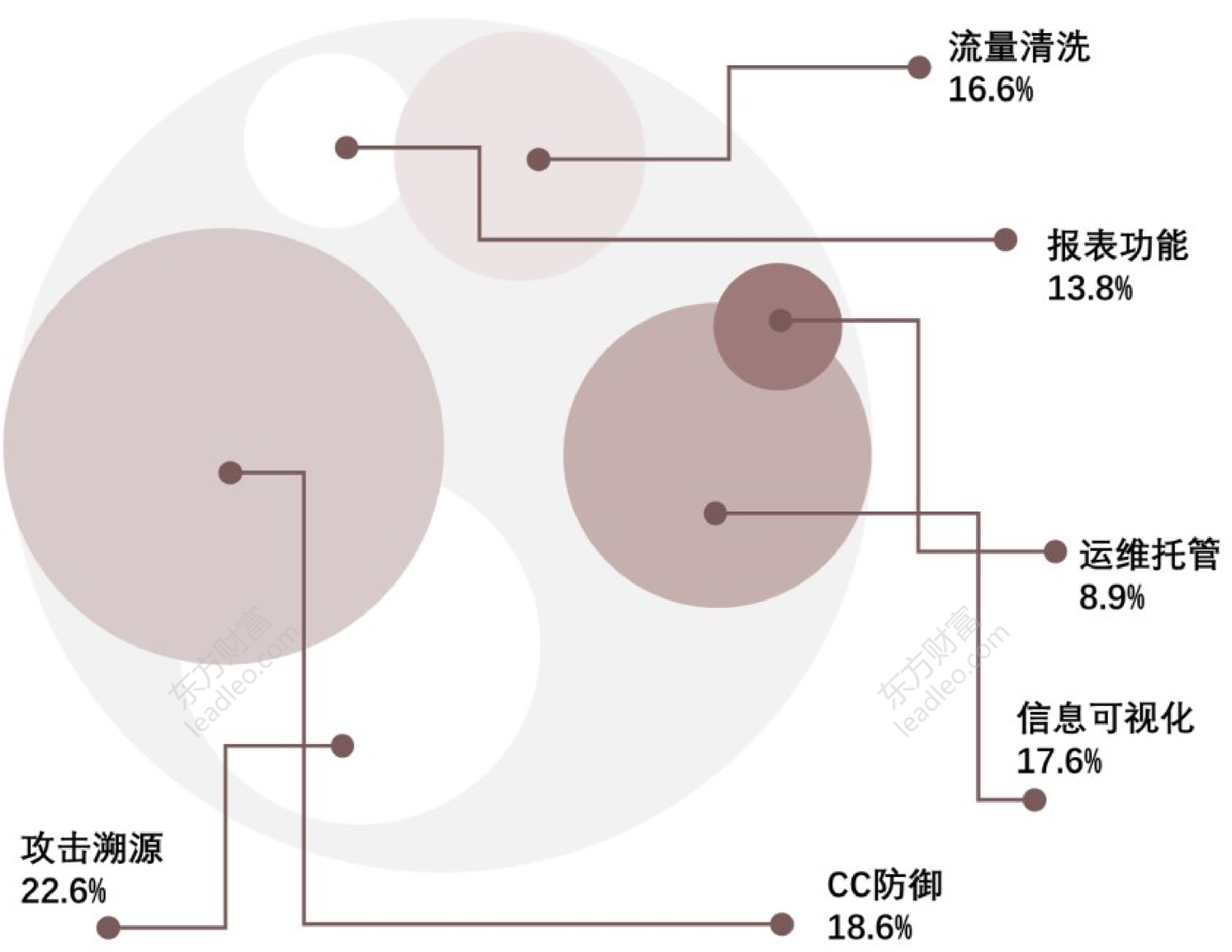
中国移动通讯，FreeBuf、IDC、头豹研究院编辑整理

云抗DDoS产品现况分析——市场关注点与产品价值亮点

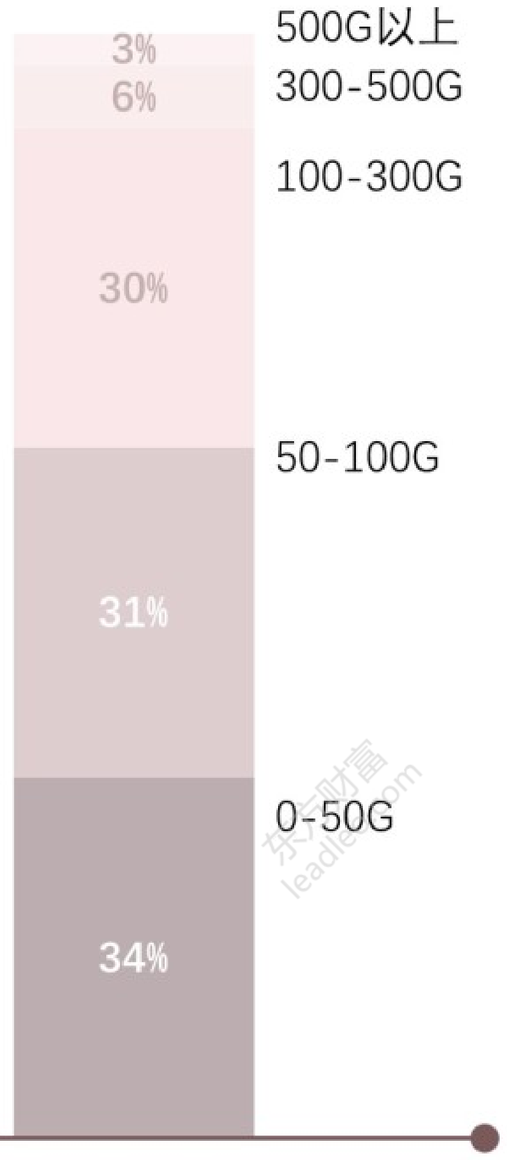
- CC防护、攻击溯源、攻击信息可视化是市场最为重点关注及期待提升的三种能力，未来有望成为抗DDoS产品与服务的市场价值亮点

抗DDoS市场关注点，2020年

产品使用反馈，2020年



DDoS攻击流量分布，2020年



❑ CC防护、攻击溯源、攻击信息可视化是市场最为重点关注及期待提升的三种能力，未来有望成为抗DDoS产品与服务的市场价值亮点

从宏观的维度看，虽然相较于2017年与2018年，中国的DDoS攻击的单次攻击流量及攻击次数均呈现双回落外事，但DDoS攻击趋势依旧严峻。根据头豹数据显示，2019年中国半数以上的互联网线上业务均经历DDos攻击。从攻击流量分布看，100G以下的小规模攻击占主流，占比超过60%。

从用户调研的维度分析，超过50%以上受调研用户表示抗D产品基本符合预期，整体满意度处于中位。但由于DDoS攻击属于技术无解型攻击方式，主要偏向于攻击缓解而非绝对防御，因此仍有10%左右用户认为现有产品能力仍存在上升空间。其中，CC防护（18.6%）、攻击攻击溯源（22.6%）、攻击信息可视化（17.6%）是市场最为重点关注及期待提升的三种能力，未来有望成为抗DDoS产品与服务的市场价值亮点。

网宿科技，FreeBuf、头豹研究院编辑整理

方法论

- 头豹研究院布局中国市场，深入研究10大行业，54个垂直行业的市场变化，已经积累了近50万行业研究样本，完成近10,000多个独立的研究咨询项目。
- 研究院依托中国活跃的经济环境，从社会保险、人工智能、大数据等领域着手，研究内容覆盖整个行业的发展周期，伴随着行业中企业的创立，发展，扩张，到企业走向上市及上市后的成熟期，研究院的各行业研究员探索和评估行业中多变的产业模式，企业的商业模式和运营模式，以专业的视野解读行业的沿革。
- 研究院融合传统与新型的研究方法，采用自主研发的算法，结合行业交叉的大数据，以多元化的调研方法，挖掘定量数据背后的逻辑，分析定性内容背后的观点，客观和真实地阐述行业的现状，前瞻性地预测行业未来的发展趋势，在研究院的每一份研究报告中，完整地呈现行业的过去，现在和未来。
- 研究院密切关注行业发展最新动向，报告内容及数据会随着行业发展、技术革新、竞争格局变化、政策法规颁布、市场调研深入，保持不断更新与优化。
- 研究院秉承匠心研究，砥砺前行的宗旨，从战略的角度分析行业，从执行的层面阅读行业，为每一个行业的报告阅读者提供值得品鉴的研究报告。

法律声明