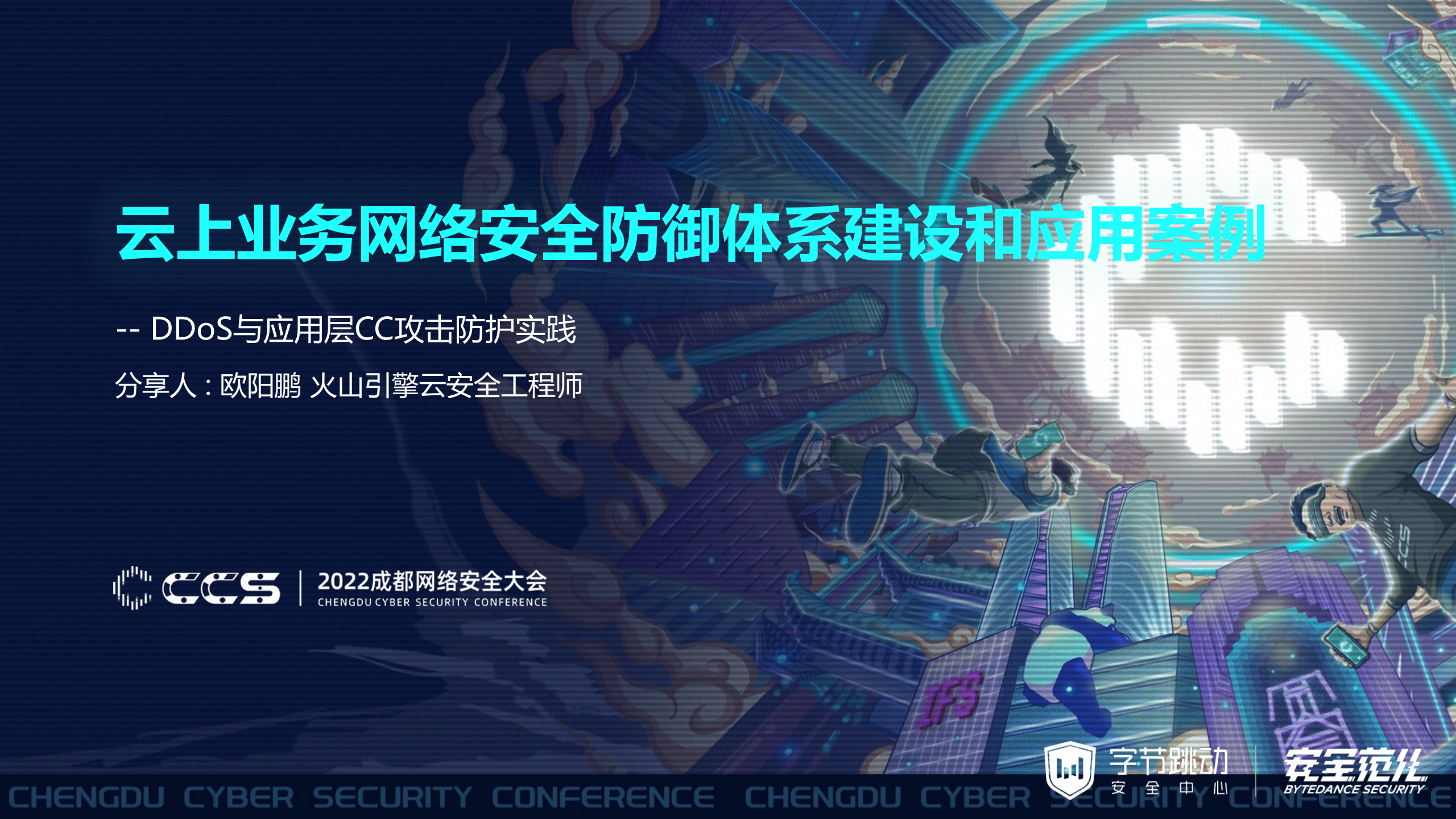
云上业务网络安全防御体系建设和应用案例

-- DDoS与应用层CC攻击防护实践

分享人：欧阳鹏 火山引擎云安全工程师

CCS | 2022成都网络安全大会
CHENGDU CYBER SECURITY CONFERENCE



字节跳动 安全中心 | 安全范化 BYTEDANCE SECURITY

- 毕业于四川大学
- 曾负责华为云WAF产品的架构设计与实施
- 负责火山引擎WAF产品的架构设计与实施
- 长期从事云上网络安全产品能力建设，专注于BOT流量分析、CC攻击防护方向

目录

- 案例背景：DDoS攻击来势汹汹，云上业务面临威胁
- 解决方案：魔高一尺，道高一丈，构建纵深防御体系
- 反思总结：优势复制，为云上业务保驾护航

DDoS攻击来势汹汹，云上业务面临威胁

业务背景

业务简介

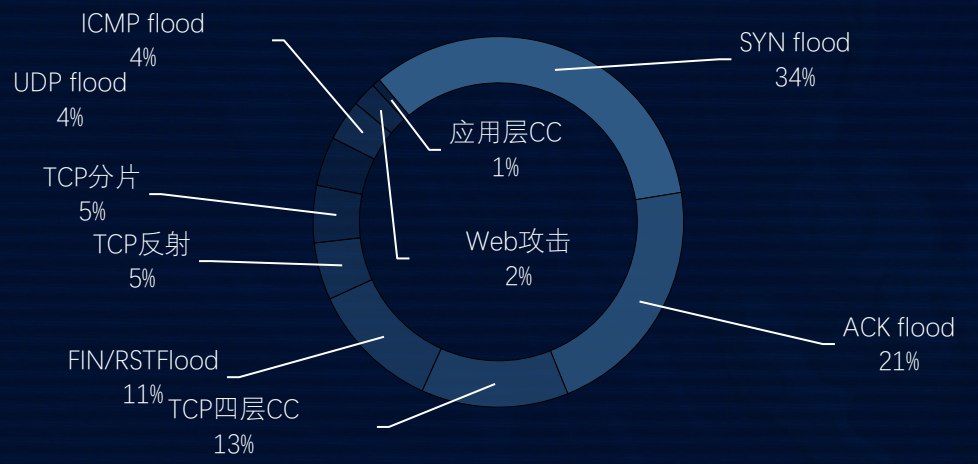
- 某网络科技有限公司，为SaaS创业公司，业务基于云上开展
- 主要为各大网站提供包括行为验证、身份验证、安全情报等安全验证服务
- 市场占有率较高，服务的目标客户企业遍布金融、直播、教育等多个领域

安全威胁

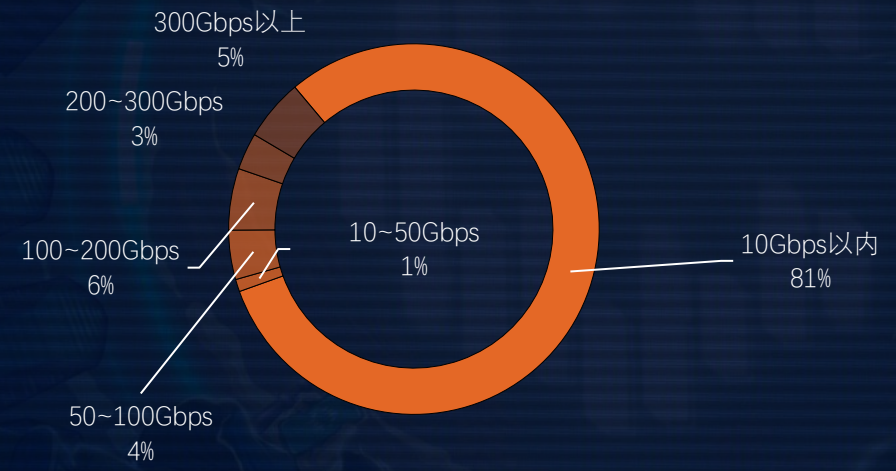
- 随着该公司市场占有率的上升及客户群体的扩大，网络安全问题也随之而来
- 面临的最显著的网络安全威胁——长期遭受DDoS和应用层CC攻击
- 攻击多次导致业务中断、瘫痪，严重影响业务运营，损害了产品口碑和收入

项目难点

攻击手法分布



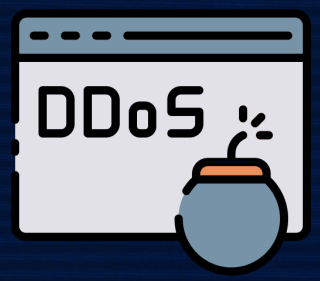
攻击带宽分布



- 攻击手法多样，防护算法必须足够精细，兼容各类特殊场景
- 攻击频繁，大流量攻击呈增长趋势，亟需超大的防护带宽以及全面的防护能力
- 必须提供优质的网络链路和高性能、高可靠的防护服务
- 防护策略必须有效覆盖现网所有网络攻击类型，包括业界难以防护的攻击手法

业务痛点

有效应对大规模DDoS/CC攻击



客户频繁遭受百G以上大规模DDoS、应用层CC攻击；所以，有效防护这些攻击是首要需求

业务场景特殊，需要自定义策略

业务场景非常丰富，且部分业务逻辑特殊，不兼容传统算法，对自定义策略需求高

业务并发量大，且对网络质量敏感

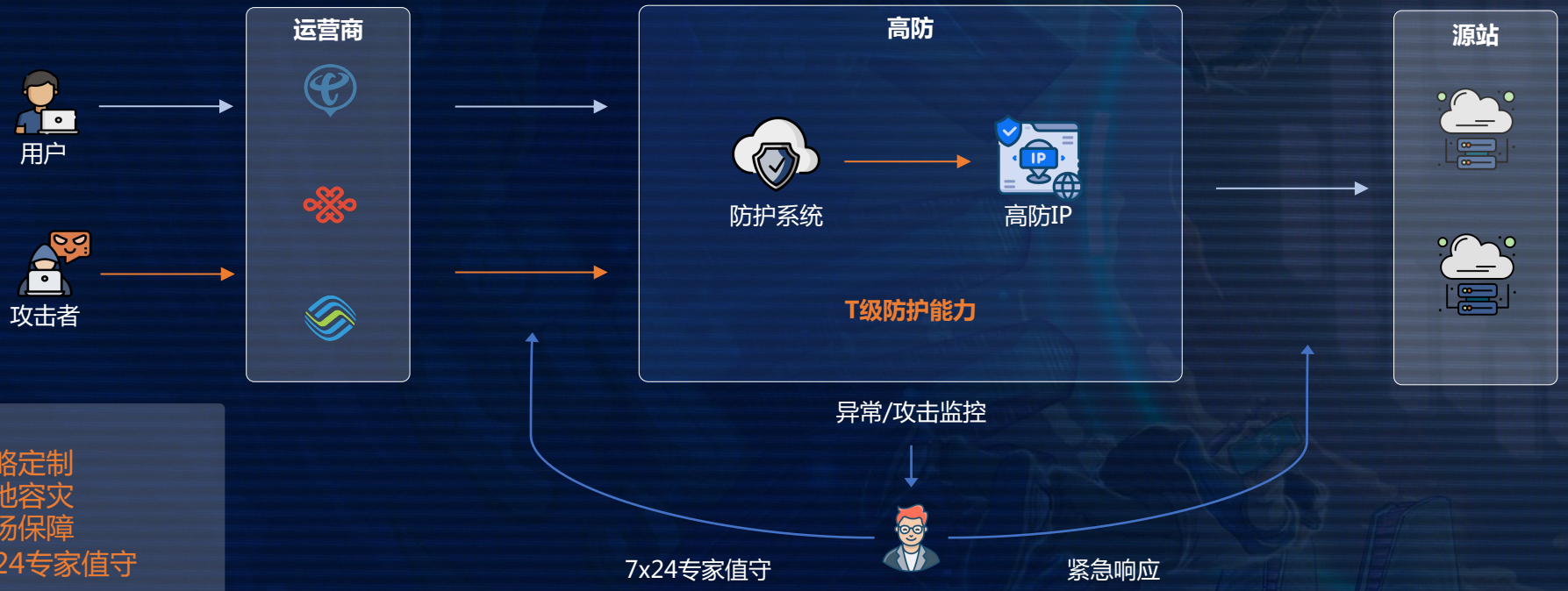
业务并发量大，且用户对网络访问质量非常敏感，所以对网络质量、防护性能要求高

攻击具有针对性和对抗性

攻击者明显具有极强专业性和目的性，所以要求防护方具备丰富的攻防能力

魔高一尺，道高一丈，构建纵深防御体系

整体解决方案



- 策略定制
- 多地容灾
- 驻场保障
- 7x24专家值守

- 借助火山引擎T级防护能力的高防IP，业务流量切到高防IP后，用户和攻击者的请求流量会经过各运营商线路接入至火山引擎网络安全系统
- 经过高防IP的流量处理，攻击流量被清洗、过滤，正常流量回注到源站，最终完成整个DDoS防护过程。

纵深防御体系

- 通过修改业务域名解析，将业务流量牵引至火山引擎提供的高防IP上，所有流量会先经过火山引擎的网络安全系统；系统对流量进行分析和清洗，最终实现攻击流量被拦截，正常业务流量转发至服务端，保障服务端安全。
- 火山引擎网络安全系统内部采用了自主研发的DDoS、WAF等防护产品组成的多层防御系统，对3~7层的攻击流量进行分层而治，并提供完备的可视化数据和安全事件告警能力。

亮点与创新

海量带宽，T级防护

依托海量带宽储备资源与优质的BGP线路，为客户提供T级的BGP DDoS防护能力，让业务免遭大规模攻击的同时享受优质的网络质量。同时支持实时弹性扩容以及自定义策略，满足不同业务场景的需求

多层防御，分层而治

基于自主研发的防护引擎而搭建多层的防御体系，对不同场景的攻击流量分层而治，从而提高了系统的防护性能以及可靠性。而且通过引入流量转发引擎，可以减少业务攻击面实现更好的防护效果

算法创新，精准清洗

自主研发了业界领先的新型防护算法，例如TCP四层CC防护模型、TCP反射算法、应用层CC多维策略等，并结合其他传统防护策略有效覆盖现网各类攻击，同时提供优质的防护体验

防护效果

- 接入火山引擎网络安全系统前，用户遭受攻击后服务崩溃，业务中断，产品口碑和收入均受到严重影响。

- 接入火山引擎网络安全系统后，累计为用户防护网络攻击90+次，包括10+次100Gbps以上的大规模DDoS攻击，峰值>300Gbps；而在攻击手法上攻击者使用了包括SYN flood、ACK flood在内的多种攻击手法，其中也不乏TCP四层CC、TCP反射和应用层CC攻击等业界难以防护的攻击手法。这些攻击均被火山引擎网络安全系统有效防护，保障了业务的稳定运行。

反思总结，优势复制，为云上业务保驾护航

防护总结

贴身策略定制

- 内置四层DDoS防护策略
- 高防IP内置防护能力
- 贴身定制的四层DDoS防护策略
- 贴身定制的七层CC防护策略

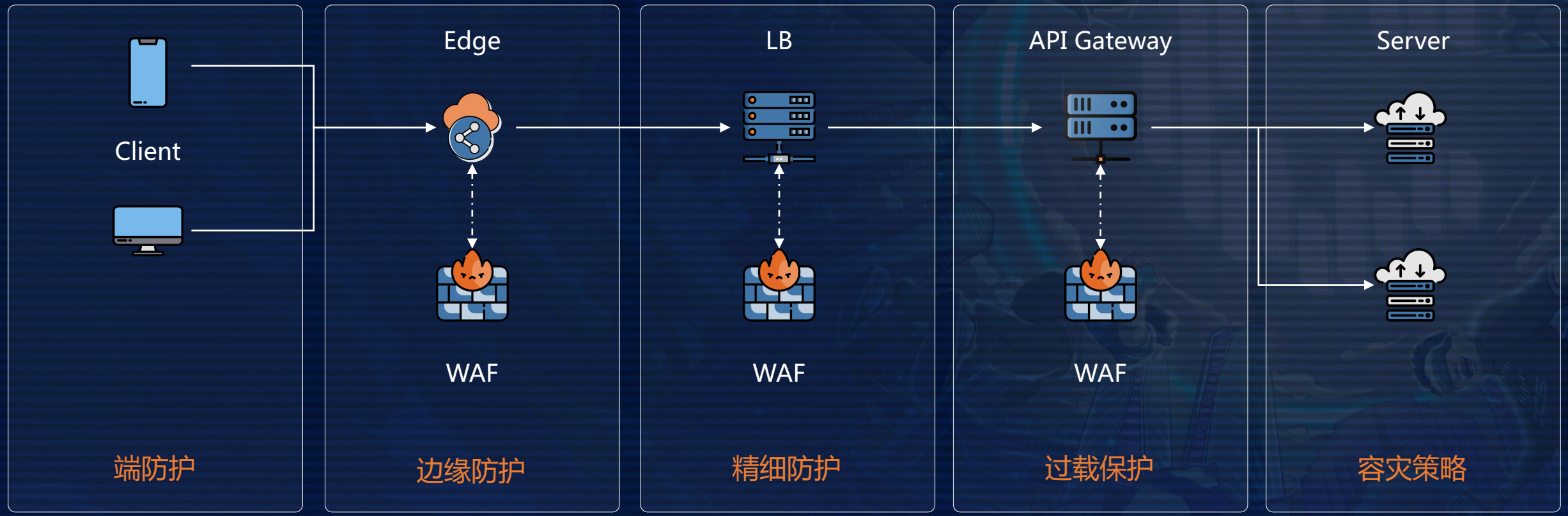
立足业务场景

- 基于攻击频次与攻击规模给出最佳防护方案
- 适配业务底层协议
- 节约业务防护成本

实现攻击溯源

- 防护数据可视化
- 人工+智能 数据分析
- 7x24 专家服务

应用层CC防护


Client
Edge
WAF
LB
WAF
API Gateway
WAF
Server
端防护
边缘防护
精细防护
过载保护
容灾策略

应用层CC防护

优势复制

01 先进全面的防护架构

- 有效提升企业在网络安全场景的防护能力
- 解决企业在网络攻击防护过程中资源不足、对抗能力薄弱、防护场景覆盖不够等瓶颈
- 具有很强的实用价值和广泛的应用场景

02 灵活兼容的防护方案

- 分层防御体系
- 灵活的自定义策略能力
- 兼容各类业务场景和需求，具有很好的可复制性以及兼容性。

03 感知、防护、管理一体化

- 流量实时自动分析
- 秒级检测和自动防护各类网络攻击流量，将业务受损程度降到最低
- 提供丰富的可视化报表和安全事件详细信息，让业务对安全攻防情况了如指掌

火山引擎


CCS
2022成都网络安全大会
CHENGDU CYBER SECURITY CONFERENCE
THANKS
CHENGDU CYBER SECURITY CONFERENCE CHENGDU CYBER SECURITY CONFERENCE