DDoS防护创新方案

# DDOS终极防护—游戏盾

DDOS PROTECTION

# 目录

# DDoS攻击现状

01

## 攻击峰值不断提高

- 2018年3月一起Memcached DDoS攻击，峰值达1.7 Tbps，标志着DDoS攻击T级时代已经来临。

02

## CC攻击越来越精细化

- IDC、PC、IoT、移动端，深度模拟业务数据发起攻击；
- 低频攻击防御难度大。

03

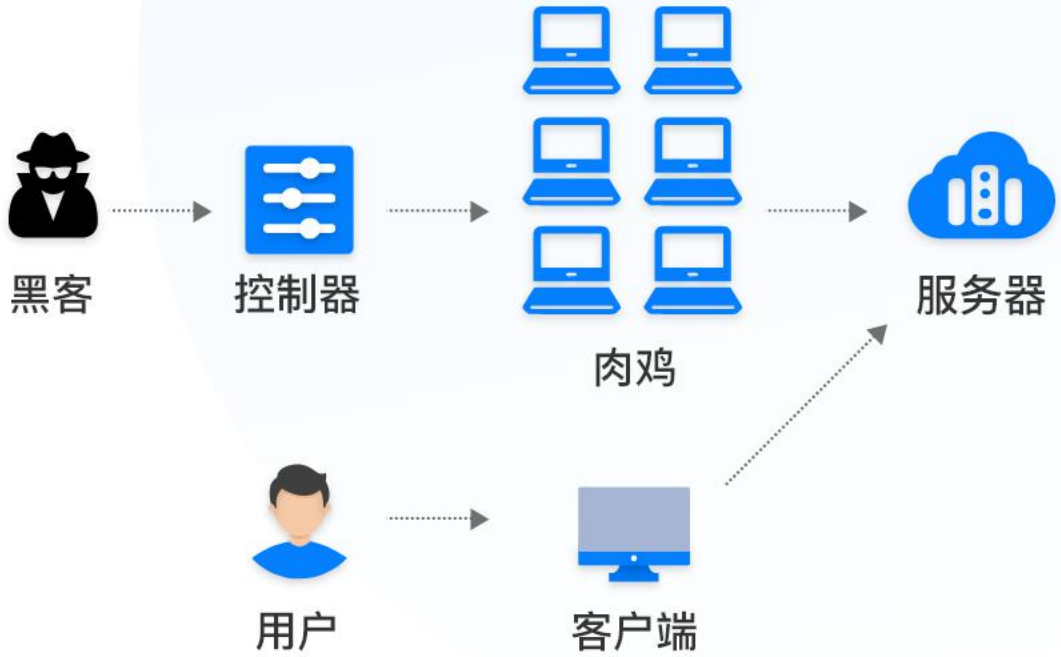
## 游戏行业仍然为DDOS首先对象

- DDoS攻击的首选对象依然是游戏行业，手机游戏更加是主要攻击目标。

04

## 攻击峰值不断提高

- 2018年3月一起Memcached DDoS攻击，峰值达1.7 Tbps，标志着DDoS攻击T级时代已经来临。



# 传统防护不足

Inadequate protection

## 防护节点有限，单节点防护能力有限

- 防护节点数量有限，攻防资源严重不对等；
- 抗海量攻击能力有限，大攻击情况下，节点稳定性差；
- 节点调度分配集中化，节点宕机切换延迟高，对客户业务影响面大；

## 防护方法单一、防护成本高

- CC粗颗粒度防护，依赖人工设置防护策略，漏防、误防严重；
- 防护能力依赖带宽大小和清洗能力，防护成本高；

## DNS解析风险高

- 依赖DNS解析，生效慢，缓存机制下节点切换延迟高；
- 通过DNS解析，节点被暴露，更有DNS解析劫持、查询攻击风险；

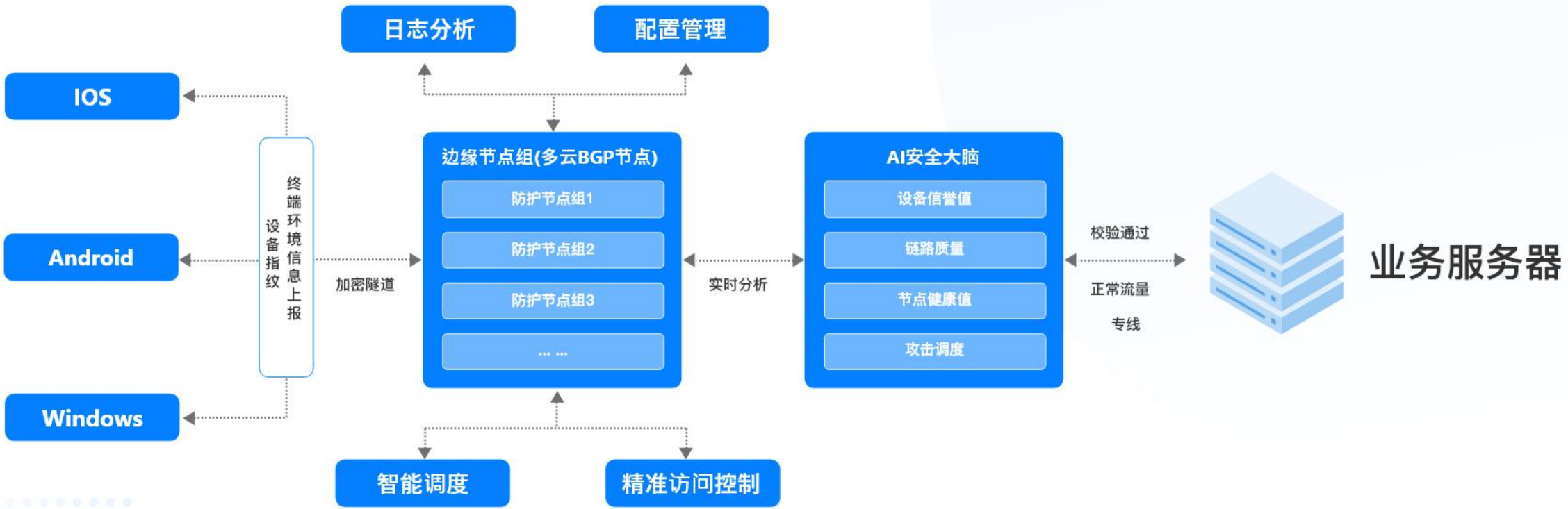
## CC防护能力相对薄弱

- 误防漏防，业务频繁掉线；
- 协议私有，无通用防护方法

# 抗DDOS方案架构



以全新算法、终端风险检测、大数据分析技术、海量分布式节点为基础，为游戏、金融、电商等行业APP应用推出的端安全解决方案。



# 抗DDOS新想法—基于SDK的防护方案一




## 隐藏攻击目标

- SDK内置默认代理IP，通过调度系统分配节点，同时隐藏节点和源站；

## DDOS防护

- 智能识别终端设备信誉等级，自动分组调度，有效识别风险设备并隔离，实战成功抵御超大型DDoS攻击；
- 创新的端边云一体架构将传统单一的硬件+硬性资源对抗 转移到了 多维度软件+弹性资源对抗。

## 智能风控调度

- 从分布式节点中就近调度，保证高质量的防护速度及链路，有效提升APP访问速度，提升访客体验；
- AI安全大脑实时分析设备信誉，链路质量，根据节点负载、可用性等进行攻击调度、拥塞调度，节点切换秒级生效；
- 区别对待真正访客和黑客，将不同流量引至不同节点组或虚拟节点，设备指纹唯一，可实现攻击设备回溯，攻击溯源。

## 高防资源兜底

- 硬性带宽资源储备，即使节点被攻击也可无限兜底对抗；

# 抗DDOS新想法—基于SDK的防护方案二




## 免疫CC攻击

- SDK与防护节点建立加密隧道，接管客户端与服务端的网络连接，使用自研加密算法对数据进行加密，对每一个TCP连接进行身份认证，丢弃未通过验证的非法连接，100%防御CC攻击。

## 高精度防护

- 黑客攻击一次后，攻击IP将被精确识别，攻击设备和IP将不再可用，打破防护资源不对称问题，具备0漏防、0误伤的精准防护能力。

## 数据安全

- 建立加密隧道，加密传输数据，攻击者无法抓包获取业务相关数据，无法进行伪造和重放攻击请求，保证数据连接的合法性，杜绝非法流量，数据加密防止数据被监听、被嗅探。

## 全网安全加速

- 全球1000+多云BGP节点，实现就近网络节点接入，结合智能选路、UDP多路传输、拥塞调度、全球加速等技术，实现APP全球访问加速。

# 抗DDOS新想法—基于SDK的防护方案三




## 终端环境检测

- 多终端自动适应，深度优化多种协议，全面检测终端环境中的风险行为，自定义规则处理，实现精准访问控制。

## 风险类型全面

- 精准识别调试/注入/Hook/DUMP、设备篡改、系统Root、网络环境、App篡改、模拟器运行、多开运行、群控运行等终端环境风险。

## 精准访问控制

- 支持IP、访客区域、设备指纹、终端系统、终端风险类型、单设备请求频率、CPU架构、设备名、应用名称、应用签名、请求端口等进行精准访问控制，根据业务情况制定专有防护策略。

## 多版本SDK

- IOS、Andorid、Windows多终端适应。

01

## DDoS无限防

传统DDoS防御依赖带宽资源对抗，节点数量有限，容易被逐一打死，节点切换延迟，大流量攻击时业务易卡顿、掉线。

安全加速SDK隐藏节点资源、动态调度、隔离风险、高防资源兜底，理论上可无限防御DDoS攻击，保障海量攻击下业务的平稳流畅。

- ★ 风险隔离
- ★ 灵活调度
- ★ 高防兜底

02

## 免疫CC攻击

传统CC防护无法快速识别CC攻击，针对低频攻击防护不佳，依赖策略防御，存在大量漏杀和误拦。

依托SDK链路加密，动态校验用户请求，拒绝非法访问，快速识别，即可响应，100%防御针对APP业务的CC攻击。

- ★ 快速识别、即刻响应
- ★ 数据加密，隐藏攻击URL
- ★ 0漏防、0误伤

03

## 延迟低

传统防护方案需要DNS解析，DNS缓存引起节点切换延迟，更有DNS劫持、DNS攻击的风险。

SDK基于全球分布式节点，结合智能选路、就近网络节点接入、UDP多路传输、全球加速等技术，取代DNS解析确保服务的低延迟和高可靠。

- ★ 取代DNS解析
- ★ 1000+多云BGP节点
- ★ 秒级生效

04

## 性价比高

传统防护方案基于攻击流量收费，DDoS攻击趋于大流量常态化，防护成本高昂。

安全加速SDK不基于流量收费，套餐内兜底防御，极具性价比，用户无差别对待，均享受全力防御保障。

- ★ 低防御成本
- ★ 高防御能力

# SDK接入步骤

Access steps

## 信息收集获取

- 了解业务详情
- 获取接入文档

01

## 平台配置

02

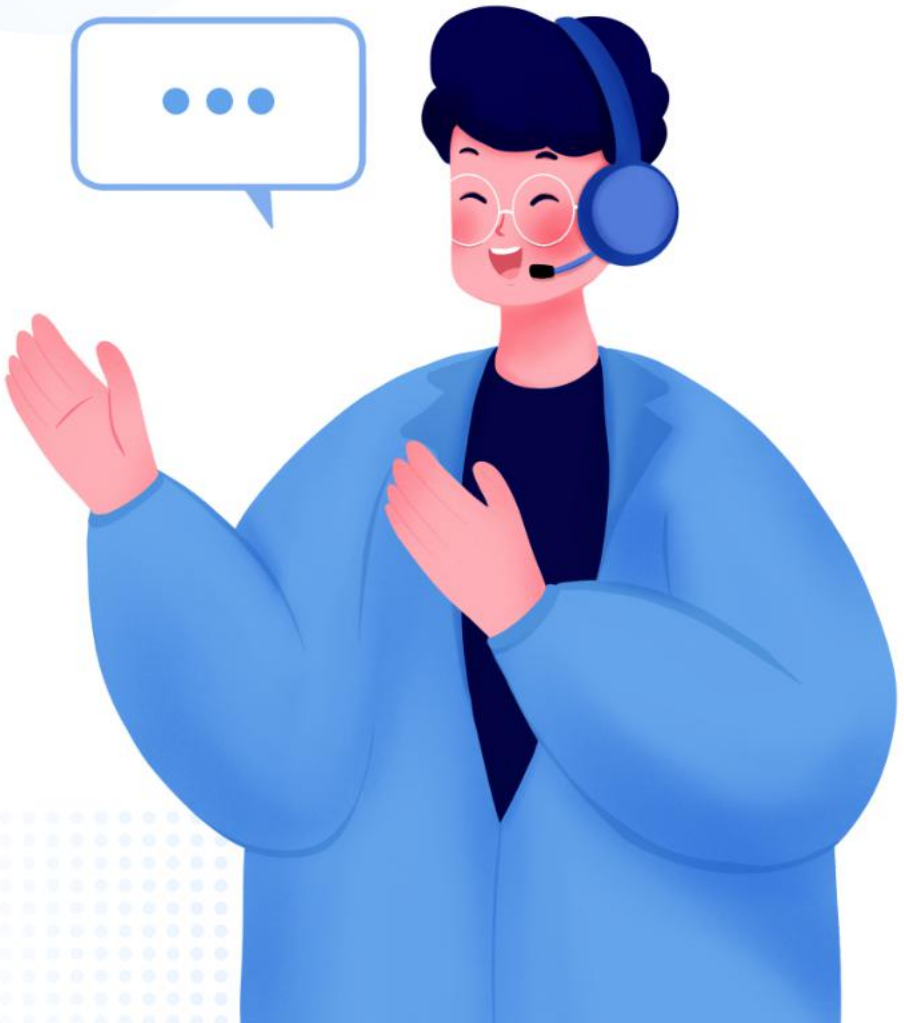
- 获取AcessKey
- 添加端口及转发规则配置

## 集成上线

- 获取SDK 并集成
- 更新上线

03

# 售后服务



**1V1专属客服经理**

为每个客户分配专属的1V1客服经理，保 障人员的文档与服务质量

**5分钟即时响应**

通过建立沟通群组，出现问题可以保证5分钟内给予用户服务响应

**7*24小时在线支持**

提供7*24小时不间断的客户问题处理服务，保障用户问题无论在何时发生，都能够第一时间介入处理

**安全专家服务**

针对特殊需求的客户提供针对性的安全专家服务