阿里云
游戏盾

产品简介

文档版本：20200113

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. **您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。**
2. **未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。**
3. **由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。**
4. **本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。**
5. **阿里云文档中所有内容，包括但不限于图片、架构设计、页面布局、文字描述，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。**
6. **如若发现本文档存在任何错误，请与阿里云取得直接联系。**

通用约定

格式	说明	样例
	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **禁止:** 重置操作将丢失用户配置数据。
	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **警告:** 重启操作将导致业务中断，恢复业务时间约十分钟。
	用于警示信息、补充说明等，是用户必须了解的内容。	 **注意:** 权重设置为0，该服务器不会再接受新请求。
	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 **说明:** 您也可以通过按Ctrl + A选中全部文件。
>	多级菜单递进。	单击设置 > 网络 > 设置网络类型。
粗体	表示按键、菜单、页面名称等UI元素。	在结果确认页面，单击**确定**。
`Courier字体`	命令。	执行`cd /d C:/window`命令，进入Windows系统文件夹。
*## *	表示参数、变量。	`bae log list --instanceid` *`Instance_ID`*
[]或者[a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{}或者{a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1 什么是游戏盾

游戏盾是阿里云针对游戏行业面对的DDoS、CC攻击推出的针对性的网络安全解决方案，相比高防IP，除了能针对大型DDoS攻击（T级别）进行有效防御外，还具备彻底解决游戏行业特有的TCP协议的CC攻击问题能力，防护成本更低，效果更好！

2017年3月29日，阿里云云盾在深圳云栖大会发布了游戏行业安全风控新模式：游戏盾。游戏盾在风险治理方式、算法技术上全面革新，帮助游戏行业用户用更低的成本缓解超大流量攻击和CC攻击，解决以往的攻防框架中资源不对等的问题。

与传统单点防御DDoS防御方案相比，游戏盾用数据和算法来实现智能调度，将“正常玩家”流量和“黑客攻击”流量快速分流至不同的节点，最大限度缓解大流量攻击；通过端到端加密，让模拟用户行为的小流量攻击也无法到达客户端。

同时，在传统防御中，黑客很容易锁定攻击目标IP，在攻击过程中受损非常小。而游戏盾的智能调度和识别，可让用户“隐形”，让黑客“显形” —— 每一次攻击都会让黑客受损一次，攻击设备和肉鸡不再重复可用。颠覆以往DDoS攻防资源不对等的状况。

2 核心原理

游戏盾的核心技术是弹性安全网络技术，简单地说，弹性安全网络将DDoS防御前置到网络边缘处。

概览

游戏盾提供了一个只能由SDK接入的并且免疫DDoS/CC攻击的弹性安全网络。SDK通过服务本地化代理接入游戏盾的弹性安全网络，实现玩家（Token）由具体的游戏盾网络接入点（GroupName）访问防护目标（Dip）端口（Dport）的逻辑。

接口示例：`YunCeng.getProxyTcpByDomain(Token, GroupName, Dip, Dport)`

表 2-1: 参数说明

名称	描述
Token	游戏内的玩家标识。发生DDoS攻击时定位恶意玩家/黑客使用，若未定义可以设置为Default。
GroupName	游戏业务对应的节点组标识，例如：access.v812vCOE21.ftnormal01al.com。在游戏盾控制台添加游戏和业务时需要配置节点组，根据游戏同时在线用户规模分配独享节点数量。一个游戏对应多个节点组。
Dip	需要转化的远端服务器的IP，在游戏盾无限抗防护目标处配置获取。
Dport	服务器的业务端口，按实际需要传入，无需在游戏盾中配置。

接入效果

通过服务SDK提供的服务本地化接口，将任意IP、端口的服务本地化，并且由SDK接管所有的通信流量，进行调度和加密传输，满足抗D、防C、流量加密等业务需求。

不同协议的接入效果如下：

协议类型	直连服务器	游戏盾本地化后
TCP	tcp://1.1.1.1:8080	tcp://127.0.0.1:8729（端口随机）
HTTP	http://www.test.com	http://127.0.0.1:2892（端口随机）

协议类型	直连服务器	游戏盾本地化后
HTTPS	https://www.test.com	https://127.0.0.1:2892（证书校验失败）-> https://www-yxd.test.com:2892 **说明:** 通过一个域名（例如，www-yxd.test.com）解决HOST匹配/HTTPS证书校验问题。更多信息，请参见#unique_5。
WS协议	ws://1.1.1.1:88	ws://127.0.0.1:2891（端口随机）

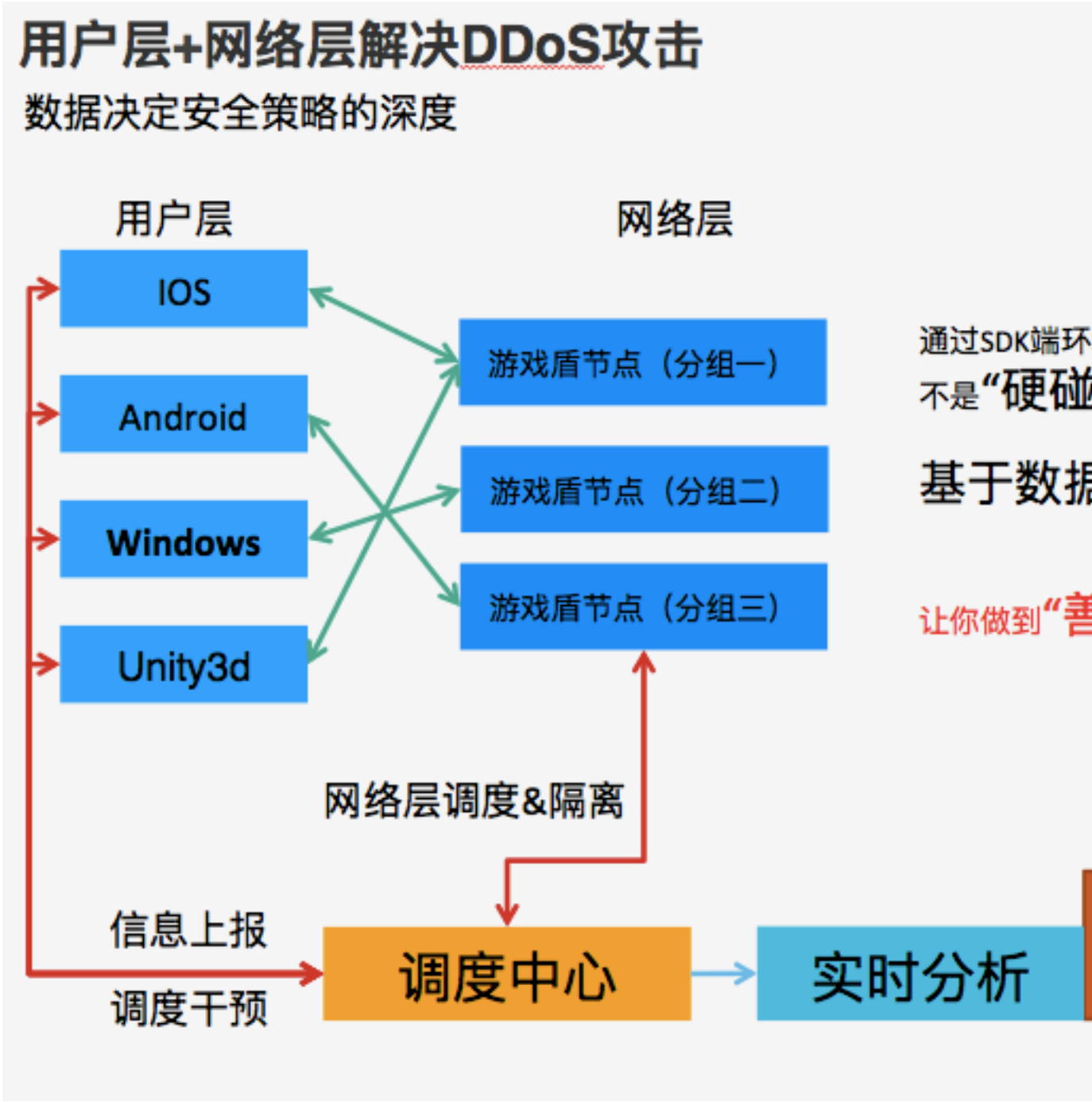
3 产品架构

游戏盾是阿里云DDoS高防IP产品系列中针对游戏行业的安全解决方案。游戏盾专为游戏行业定制，针对性解决游戏行业中复杂的DDoS攻击、游戏CC攻击等问题。

游戏盾由两大模块组成：

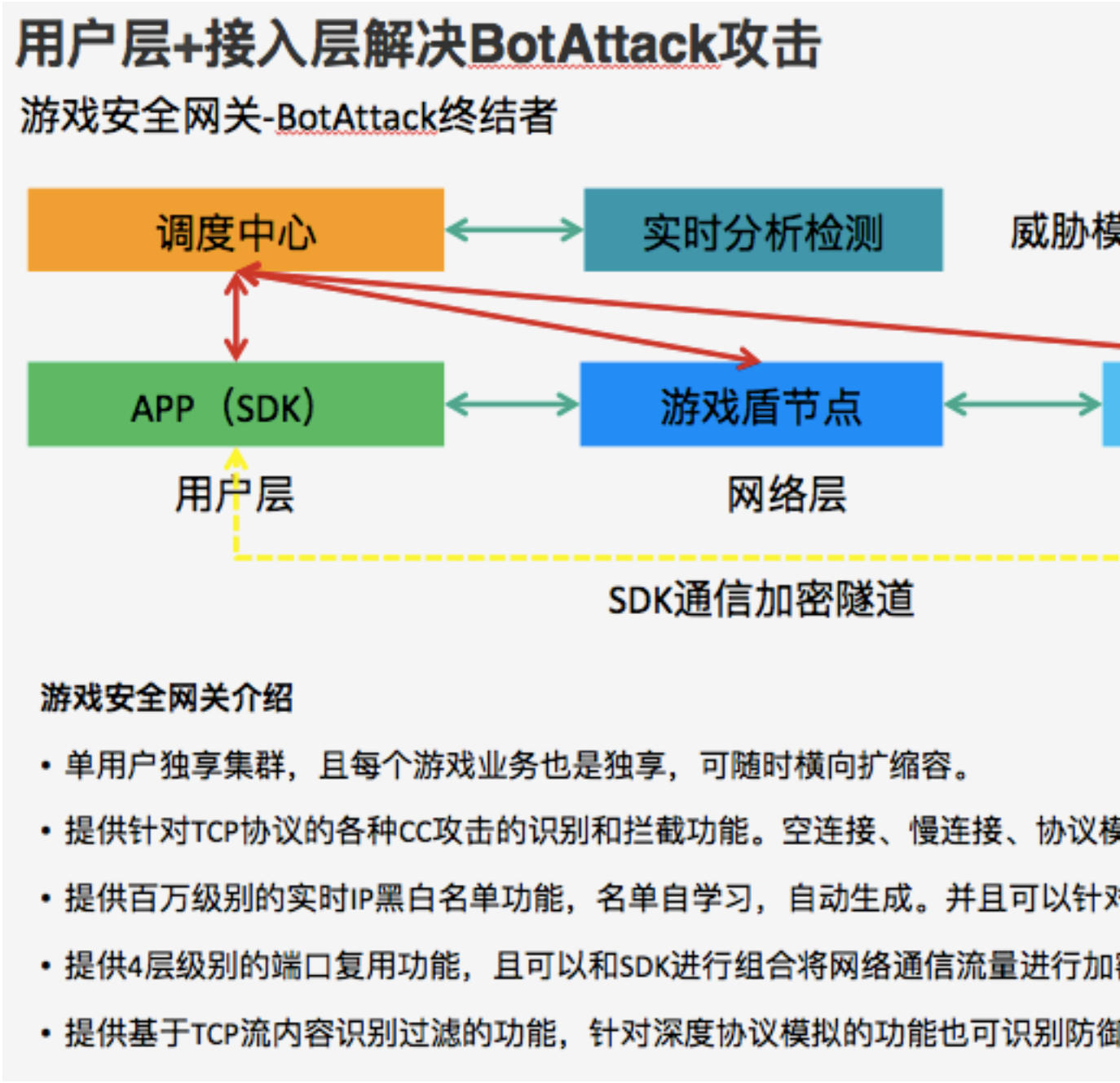
- 分布式抗D节点：通过分布式的抗D节点，游戏盾可以做到防御600G以上的攻击。
- 游戏安全网关：通过针对私有协议的解码，支持防御游戏行业特有的CC攻击。

游戏盾防御DDoS攻击的原理



与普通的DDoS高防机房不同，游戏盾并不是通过海量的带宽硬抗攻击，而是通过分布式的抗D节点，将黑客的攻击进行有效的拆分和调度，使得攻击无法集中到某一个点上。同时基于SDK端数据、流量数据，可以通过动态的调度策略将黑客隔离！

游戏盾防御CC攻击的原理



一般来说，游戏行业的CC攻击跟网站的CC攻击不同。网站类的CC攻击主要是基于HTTP或者HTTPS协议，协议比较规范，相对容易进行数据分析和协议分析。但是游戏行业的协议大部分是私有的或者不常见的协议，因此对于游戏类CC攻击的防御，阿里云推出了专业的云上防御游戏安全网关（原称NetGuard、简称NG）。

游戏安全网关通过在用户业务和攻击者之间建立起一道游戏业务的防火墙，根据攻击者的TCP连接行为、游戏连接后的动态信息、全流量数据，准确分辨出真正的玩家和黑客。

- 游戏安全网关支持大数据分析，根据真实用户业务的特点分析出正常的玩家行为，从而直接拦截异常的客户端（协议非法）。且可以随时针对全国省份、海外的流量进行精确封禁，支持百万级的黑白名单。
- 游戏安全网关可以同SDK建立加密通信隧道，全面接管客户端和服务端的网络通信，仅放行经过SDK和游戏安全网关鉴权的流量，彻底解决TCP协议层的CC攻击（模拟协议型攻击）。

> **说明:**
> 需要使用SDK5.1.7或以上版本。

4 功能特性-智能调度

技术革新：智能调度算法拆分流量

DDoS攻防的本质，是资源的对抗。从网络、CDN、服务器到数据库，只要存在资源差的地方，就可以有DDoS攻击在发生。

资源类别	用户	黑客
带宽资源	G级别有限的带宽和峰值触发方式的黑洞机制	T级别压倒性带宽资源
肉鸡资源	有限的服务器资源	大数量级领先的肉鸡资源
技术资源	需要防护完整的一个面	只需要击破一个点
资金资源	有限的预算+高昂的防护成本	几乎无成本

从云层、弹性安全网络到现在的游戏盾，阿里云安全团队在与游戏行业用户并肩作战几年后，用数据和算法来改变了大流量攻击防御的模式。

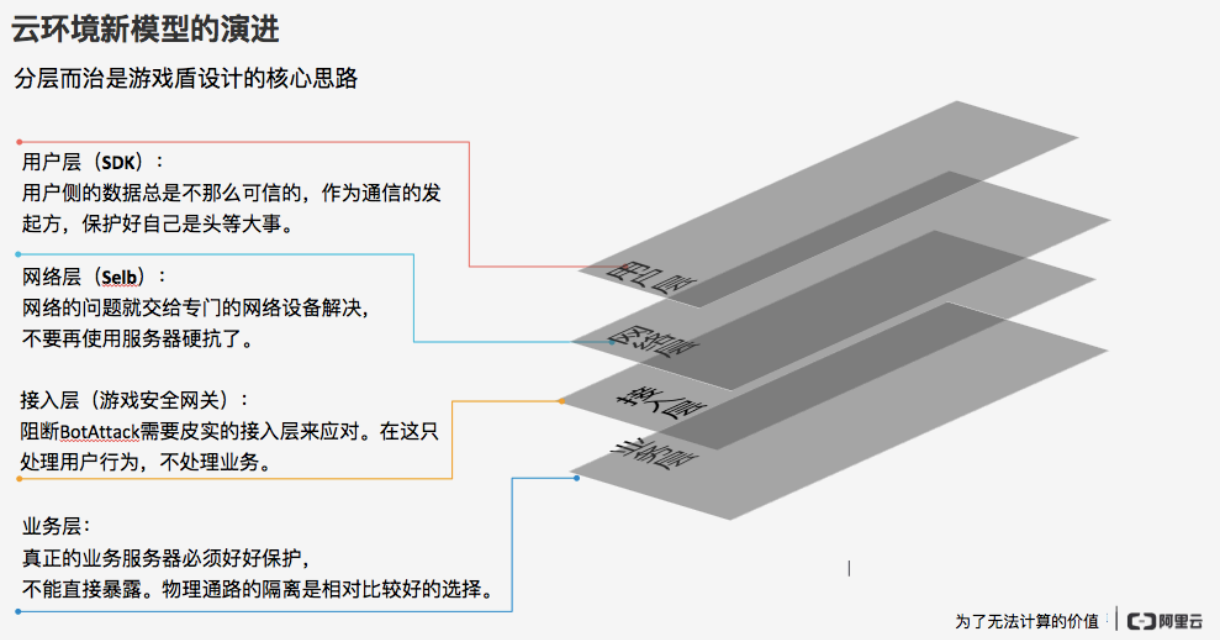
今天，游戏盾在应对黑客攻击的时候，不仅是被动在防御，也具备主动的反击能力。有效识别哪个客户端是黑客、哪个客户端是合法用户，通过更加灵活的调度算法，让用户的正常流量和黑客的攻击流量“不往一处走”，扛住一次次超大型的DDoS攻击。

在游戏盾的演进过程中，阿里云安全团队成功平衡了四大资源不对等的难题：

- **如何对抗黑客T级压倒性带宽资源。**
- **如何攻破黑客的肉鸡资源。**
- **如何填补黑客只需要“攻点”、用户需要“防面”的鸿沟。**
- **如何解决资金成本的问题。**

5 功能特性-分层而治

风控模式革新：从单点防御到分层治理



分层而治，是解决这些问题的基础。所有资源的不对等，都是因为攻击方太容易找到目标，而防御方太容易成为目标。

分层而治中的“分”，代表流量的拆分、业务的拆分、和目标的拆分；让攻击者的成本和门槛增大，把用户成本控制到最低；“层”代表一种漏斗模型。以前，我们都是用带宽去硬抗DDoS攻击，而在游戏盾中，我们用最适合的‘武器’去做最擅长的事。

- **用户层（SDK）：用户层的数据总是不那么可信的，作为通信的发起方，保护好自己是头等大事。**
- **网络层（Selb）：网络的问题就交给专门的网络设备解决，不要再使用服务器硬扛了。**
- **接入层（游戏安全网关）：还记得CC攻击的影响吗？接入层就是为了应对它准备的。在这一层，只处理用户行为，不处理业务。**
- **业务层：真正的业务服务器必须好好保护，不能直接暴露，物理通路的隔离是相对比较好的选择。**

游戏盾改变了DDoS攻防只是“拼带宽”的传统概念，成为针对游戏行业用户的整体风控方案。在游戏盾的风控理论下，只要我们解决好用户端的问题，就可以解决无限大的DDoS攻击，从而达到攻防成本的平衡。

6 产品优势

对比项	游戏盾	传统DDoS流量清洗机房
游戏行业超大DDoS攻击	摆脱DDoS攻防军备竞赛，专业防御游戏行业超大DDoS攻击分布式抗D节点优质BGP接入，针对游戏提供高可用的网络环境	仅能靠一个本地机房，带宽无法扩展，无法防御更大的DDoS攻击
指纹加密/链路加密	支持TCP/HTTP/HTTPS适合手游、端游等各类业务场景支持云内/云外客户集成游戏SDK，数据报文全链路加密，防黑客破解端到端的加密，游戏安全接入支持防护针对模拟游戏协议的攻击支持解码游戏私有协议防护算法实时调整	传统清洗机房仅靠硬件设备来识别，无法解码游戏私有协议
支持解码游戏私有协议	DPI深度报文检测技术，通过机器学习自动建立协议特征，仅放行满足协议特征请求	传统清洗机房仅靠硬件设备来识别，无法解码游戏私有协议
定制游戏防护算法	防御游戏空连接、慢连接、恶意踢人攻击全球僵尸网络库、神盾局攻击溯源	传统机房大多采购防火墙设备或者硬件设备，防御算法更新慢，自身没有调整防御算法的能力

说明:

您必须单独购买Web应用防火墙，才能获得HTTP/HTTPS协议的CC防护支持。

7 发展历史

游戏盾的前世今生

游戏盾从诞生之初到现在，经历了三次重大的技术变革。从初代的“云层”，到现在的游戏盾，无论是从技术架构还是从功能实现上，都发生了翻天覆地的变化。

而驱动这些变化的浅层因素，是攻防资源的不对等问题；深层因素则是对现有网络本身的路由规则和基础设施的深度思索。

简单来说，游戏盾通过风控模式调度流量来撬动攻防天平；而从本质来说，游戏盾更像是一个除了路由和DNS之外，能够再次改变流量走向的存在。

云层：第一次实验

游戏盾的前身是云层项目。它诞生在2015年初的一次“营救实验”。

一家公司遭受黑客的反复攻击，传统的DDoS防御方法已全部败下阵来。在紧急情况下，公司向阿里云安全团队寻求合作，并提出可以尝试一种“通过快速流量调度，来躲避黑客攻击”的新方法。

当时，这种方法并没有在任何实战场景中被验证过。阿里云DDoS防护安全技术团队在“摸着石头过河”的情况下，与用户的技术团队一起合作，将这种新的防护方法付诸于实践，成功扛下了一次次攻击。

云层时代也就此开始。

当时，黑客的攻击手法相对来说比较单一，找到目标IP地址，通过一波大流量（10~50GBps）攻击将IP打进黑洞。而黑客发动下一波攻击的准备时间大约需要10~15分钟。而云层通过秒级分布式IP的快速调度，压制了黑客的分钟级攻击跟随，赢得了这场竞赛的阶段性胜利。

接下来，“云层”模式在其它几场攻防实战中屡立战功。但与此同时，新形态的攻击方式也在不断地进化，云层尽管实现了秒级的IP调度速度，但要跟上黑客的嗅探和跟随，其算法和效率仍然需要进化。在这种背景下，游戏盾的时代来了！

游戏盾：正式踏入战场

一直以来，中国超过50%的DDoS和CC攻击，都是针对游戏行业。因此，游戏成了DDoS攻防最好的战场，也是调度算法的最佳训练场。

于是，阿里云安全团队决定将云层时代积累下来的技术经验，应用在游戏行业中，成为所有用户能够用得上、并且管用的风控模式。

在游戏盾诞生之前的很长一段时间，阿里云安全团队对游戏行业的攻防对抗模式反复分析，深入了解了游戏业务的注册特点、登录特点、玩家特点，并在此基础上重构了游戏盾的智能调度算法。

游戏盾继承了云层快速调度的能力，又通过对端信息的采集、和对网络通信等行为进行归一化的处理分析。基于云上的资源和特性，游戏盾得以对海量的端数据进行计算、处理和存储；相比线下环境，借助云计算平台在计算和数据处理上的优势，阿里云取得了实质性的突破——完成对每一个终端设备的画像，并最终沉淀为“端威胁值”这一新的调度因子。

游戏盾所有数据处理的核心是空中流量调度系统（AirTraffic Control，ATC），它以深度机器学习（DL）和神经网络（LSTM）为认知基础，将恶意用户快速隔离在调度体系之外。

在游戏行业炮火重重的前线上，游戏盾完成了涅槃重生，并在最猛烈的攻击之下不断进行自我升级。同时，威胁识别和影响面控制代替调度成为了新的技术关键词。

精细化和分层而治：领先一小步

当然，这仍只是一个开始。攻击方也在逐步加重自己的兵力投入。想要领先黑客一小步，光靠数据和算法还不够，需要真正了解对方的攻击趋势和攻击手法。

在实战的磨砺中，游戏盾正式踏入精细化攻防对抗这一领域：NetGuard应运而生。

借助前两个阶段所积累的AI建模分析能力，游戏盾向针对业务层的攻击发起挑战。

游戏盾通过串行学习特定业务数据特征，快速识别畸形和突发的异常流量，并在干路上进行阻截。与此同时，阿里云安全团队提出了由用户层、网络层、接入层和业务层四级联动的立体防护体系，让游戏盾帮助用户搭建最适合自己的安全架构。

游戏盾的立体防护体系的核心，在于分层而治。首先，大流量攻击依托网络层去解决；而技巧型CC攻击通过接入层去解决。立体防护体系可以达到突破带宽限制，控制攻击影响范围和时间，精准识别用户行为的目标。

倾斜的天平

从2015到2017，经过两年的攻防实战和技术打磨让游戏盾将一种新的安全风控模式，应用到攻防战场中，帮助游戏行业的用户去解决实质性的问题。

然而，从云层到游戏盾，只是阿里云安全团队撬动DDoS攻防天平的第一步。真正前进的方向，是构筑一张安全、可信、承载着“干净流量”的网络，并将这张网络延展到更广的边界。