

## 目录

目录	1
产品概述	2
DDoS原生高防的使用对象	2
DDoS原生高防解决的痛点	2
技术原理	2
产品优势	2
一键防护	2
双协议防护	2
降低成本	2
定制化防护	2
使用场景	2
大流量DDoS攻击	2
托管机房全段防护	2
使用须知	2
支持地域列表	2
IP限制	3
业务带宽限制	3

## 产品概述

DDoS原生高防（Kingsoft Cloud Native Advanced Defense, 简称KNAD）是针对部署在金山云内业务提供DDoS防护能力的产品，通过绑定云上 IP 即可提供防护能力，免去了更换业务IP和繁琐的接入过程，具有实时防御、低延时、高可靠的特点。

### DDoS原生高防的使用对象

DDoS原生高防面向金山云内业务及金山云托管机房，无需更换IP的前提下提供原生T级DDoS攻击防护服务。

### DDoS原生高防解决的痛点

- 业务被DDoS攻击，但公有云只能提供有限的基础防护能力
- 使用云外高防需要更换业务IP，转发配置繁琐还容易出错
- 当正常的业务带宽很高时，使用云外高防会产生高额带宽费
- 使用传统高防，云外绕行导致访问质量下降

### 技术原理



## 产品优势

### 一键防护

将弹性IP绑定到DDoS原生高防即可加载高防能力，不增加网络延迟即可提供T级原生防护能力。

### 双协议防护

同时支持对IPv4和IPv6协议IP提供防护能力，满足客户双协议业务防护需求。

### 降低成本

可按月购买基础防护，按天计费弹性防护能力，灵活配置防护套餐，做到按需付费，节约成本。

### 定制化防护

根据具体需求和网络环境自定义防护策略，针对性地保护关键资源的稳定性和服务的连续性。

## 使用场景

DDoS原生高防通过绑定金山云业务IP，提供原生高防能力，受攻击无需再更换IP，并且具有较低的访问延迟，具有如下应用场景

### 大流量DDoS攻击

- 游戏、电商等容易受超大DDoS攻击防护场景
- 直播、视频等对网络访问质量要求较高的场景
- 新品发布、新游戏、促销等按需DDoS防护
- 公有云基础DDoS防护无法满足，需更高防护能力的场景

### 托管机房全段防护

- 托管机房业务被大流量DDoS攻击，扫段攻击的场景
- 托管机房出口网络设备IP被DDoS攻击的场景

## 使用须知

### 支持地域列表

当前DDoS原生高防所有支持的地域如下表所示：

地域名称	地域代码	是否支持
------	------	------

华北1（北京） cn-beijing-6 已支持

华东1（上海） cn-shanghai-2 已支持

### IP限制

单个防护实例最多绑定100个弹性IP 需绑定 DDoS\_BGP 链路EIP

### 业务带宽限制

单个防护实例业务带宽：100M--15Gbps