应用安全解决方案（APP-S） 产品白皮书V2.0

网世界 心归宿

网宿科技 全球领先的互联网基础设施平台

关注公众号，及时了解网宿产品与服务动态

400-010-0617 | www.wangsu.com

Content 目录

网宿“应用安全解决方案（Application-Security，简称 APP-S）”是“网宿网盾”品牌旗下专为各类业务应用（如金融行业的在线开户系统、行情资讯等、端游、手游等）打造的安全防御解决方案。可抵御各类突发 DDoS 攻击，保障网站在遭遇大流量 DDoS 攻击时仍然能够稳定在线，避免业务中断带来损失。同时，对正常访问提供加速服务，保障用户体验。

“网宿网盾”是网宿科技发布的云安全全新品牌，其业务全景主要覆盖网络安全、业务安全、内容安全、DNS 安全、源站可用性、传输安全、安全管理和安全评估等八大领域，“网宿网盾”依托高容量节点和自主研发的安全技术，构建出一套云端智能安全体系。

1.行业现状和挑战

随着互联网在电商、金融等领域的强力渗透，订单交易、股票行情咨询等业务应用出不穷。同时，根据《2016 中国游戏产业报告》显示，中国游戏市场实际销售收入达到 1655.7 亿元，移动游戏和客户端游戏占据游戏市场的半壁江山，分别为 49.5%和 35.2%。尤其是棋牌类游戏，在 2016 年市场井喷，市场规模达到 58.6 亿元。

由于行业的高产值、高利润，并且对业务的可用性要求高，出于黑客敲诈勒索、同行恶意竞争等因素，业务应用系统极易遭遇 DDoS 攻击。而电商、金融、游戏等行业的业务系统一旦由于 DDoS 攻击导致业务中断，将严重影响业务的正常运作，从而导致用户流失、交易失败、交易量下降等，给企业带来经济损失。各行业的业务应用主要面临以下挑战：

- **攻击频率越来越高，峰值越来越高**

随着 DDoS 攻击工具的泛滥及地下黑色产业市场的发展，DDoS 攻击门槛越来越低，且物联网设备的大力发展（但物联网设备厂商的安全意识普遍不高，其设备往往存在漏洞，极易被黑客利用成为

DDoS 攻击的工具），DDoS 攻击事件越来越频繁。根据 CNCERT 发布的《2016 年中国互联网网络安全报告》显示，2016 年大流量攻击事件数量全年持续增加，10Gbps 以上攻击事件数量第四季度日均攻全年日均达 133 次，占日均攻击事件的 29.4%，且数百 G 的攻击带宽已司空见惯。

◆ **攻击造成的损失越来越大**

DDoS 攻击将导致平台服务中断，服务中断导致的用户流失、交易量下降、网站恢复的代价、品牌形象损失等等，都应该计算到其经济损失内，甚至目前有些黑客还利用 DDoS 攻击对网站进行敲诈勒索，这些都给网站的正常运营带来极大的影响，DDoS 攻击造成的损失呈几何式增长。在网络攻击猖獗的大环境下，互联网企业频繁遭遇窘况，无法专注于业务开展和推广，形式及其严峻。

◆ **传统防护方式存在瓶颈**

为了抵御各类 DDoS 攻击，企业可能会选择购买抗 D 硬件设备或高防机房的方式来提高系统抗 DDoS 攻击。这种方法虽然能一定程度上缓解攻击，但是这两种方法存在以下不足：

1. 受限于带宽和设备性能，无法有效应对突发大流量攻击

目前市场上黑客攻击成本和门槛都很低，已经形成了产业链，同时黑客攻击手段捉摸不定，数百 G 的突发大规模攻击已是司空见惯。而传统抗 D 硬件设备的可扩展性受限于带宽和设备性能，因此当黑客骤然提高攻击流量后，传统防御方式往往失效，所以不能从根本上防护 DDoS 攻击。

2. 部署复杂，运维难度高

硬件设备一般采用串联或旁路方式部署，需要对源站的网络拓扑做变更，部署过程中存在系统和业务风险，并且加大运维难度，当设备出现问题时，难以及时解决。

◆ **业务响应慢，影响访客体验**

随着企业业务的扩展，其业务应用的访问并发越来越高，同时，跨运营商、跨区域访问频繁，而运营商针对跨网传输的内容都做了流量限制（如电信与联通之间有着数万毫秒的网络延时），将导致跨网访问的时延过高，而国内还存在一百多家小运营商，运营商互联互通问题瓶颈愈加凸显，各类问题都可能导致业务响应速度慢等现象，进而影响用户体验和办公效率。尤其是游戏行业，玩家对游戏流畅的体验需求比较高，一个体验不好的游戏将流失大量玩家。

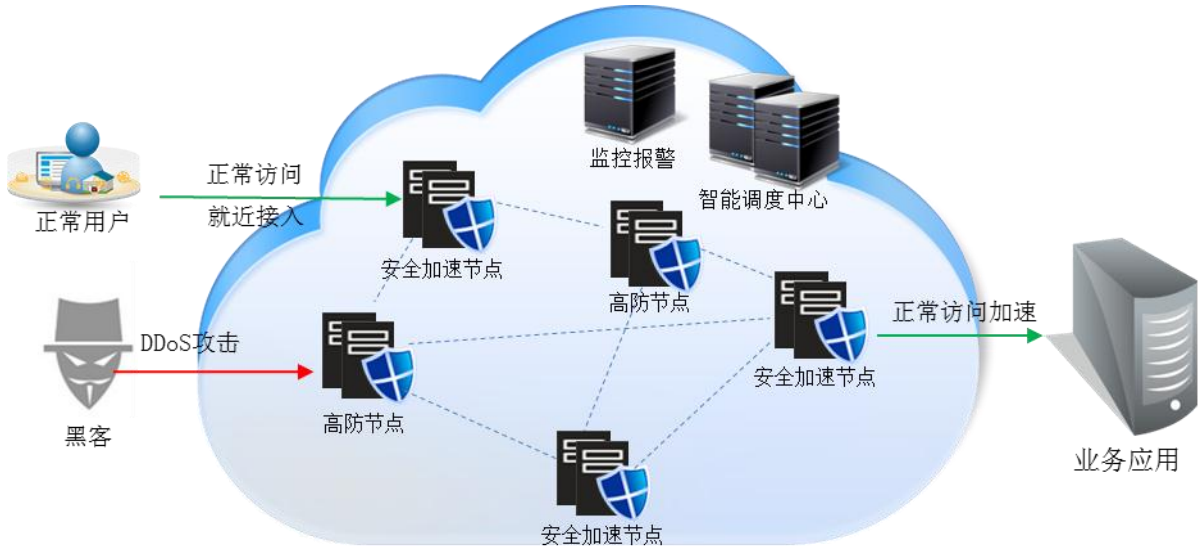
2.方案介绍

2.1.方案简介

网宿 APP-S 是基于 TCP/IP 协议组的应用系统量身打造的安全解决方案，采用先进的防御算法，依托网宿节点资源优势。 目前网宿 APP-S 单节点抗攻击能力可达 600Gbps，同时智能调度中心能够根据攻击情况智能调度全网资源，总体抗攻击能力达到 10Tbps+。

2.2.技术架构

网宿 APP-S 依托全球部署的云安全节点联接形成云安全网络，并配以专有的攻击监控报警中心和智能调度中心，实时检测分析请求包，如发现异常请求，可及时报警并拦截，同时可根据攻击情况实时动态调整防护策略，有效保障客户的业务应用安全。对于正常访问提供加速服务，提升用户访问体验。网宿 APP-S 架构如下图所示：



2.3.接入方式

网宿应用安全解决方案（APP-S）提供 IP 接入、CNAME 接入、HttpDNS 接入三种方式，客户可以根据自己的业务类型选择合适的接入方式：

- **IP 接入方式**

适用于无域名的业务。客户将其业务应用系统对外服务的 IP 更改为网宿提供的 IP。根据客户是否自有选路系统分为两种方式：

1) 如果客户自有选路系统，可以调用网宿 IP 服务列表智能选择最优节点访问。

2) 如客户自身没有选路系统，则直接绑定网宿高防 IP。存在风险：当节点故障时，无法自动切换节点，需要客户手动切换。

- **CNAME 接入方式**

适用于有域名的业务。无需客户做任何修改，客户直接将域名 CNAME 到网宿 APP-S 即可，并且当节点故障时，节点能够自动切换调度。

存在风险：这种接入方式基于 DNS 调度，可能会出现域名被劫持，解析结果跨地区、跨运营商导致业务访问慢甚至无法访问的情况。

◆ **HttpDNS 方式接入**

有无域名皆可使用。客户调用网宿提供的 HttpDNS API，并携带域名和 IP 信息向网宿 HttpDNS 服务器发起查询请求，网宿 HttpDNS 服务器基于请求域名和 IP 信息，查询 CDN 内部调度策略，得到适用该用户的最优节点。这种接入方式能够解决域名劫持等安全问题，并且当节点故障时，节点能够自动切换调度。

存在风险：需要客户端做修改，且业务应用需要有客户端。

2.4.适用行业与场景

网宿 APP-S 能够为非 HTTP/HTTPS 的业务应用系统提供 DDoS 防护服务，保证其业务不中断。网宿 APP-S 面向的行业及使用场景包括但不限于：

1. 游戏行业

游戏行业作为高产值、高利润、竞争激烈的行业，一直是黑客发起 DDoS 攻击的高发地，同时也是动辄数百 G 大流量攻击的多发行业。对于游戏行业来说，保证业务的可用性和连续性是留住玩家的前提，而 DDoS 攻击恰恰是对可用性和连续性的最大威胁。

场景：手游、端游的游戏端口（如人物选择端口、房间端口）、游戏过程……

2. 金融行业

金融行业（银行、证券、基金、股票等）向来是黑客觊觎的“钱袋子”，且同行竞争也非常激烈。金融行业对业务可用性要求非常高，而一旦发生业务中断，正常用户无法进行交易下单，将造成严重的经济损失。

场景：手机银行、在线支付系统、证券交易系统、股票行情系统、在线开户系统……

3. 企业信息化系统

业务管理系统关系着企业的正常运作。因此，黑客出于敲诈勒索或同行恶意竞争等因素，企业业务管理系统极易遭受 DDoS 攻击，而一旦遭受攻击，以 ERP 系统为例，将出现大量用户不能发货、订单提交失败等问题，造成大量的经济损失。

场景：云 ERP、云 CRM……

3. APP-S 功能

网宿 APP-S 提供监控报警（包括攻击监控报警、业务可用性监控和节点服务质量监控）、流量型 DDoS 攻击防护、空连接防护、类 CC 攻击防护、防护报表展示等功能，从而保障各应用系统的服务实时在线。

3.1.监控报警

APP-S 为客户提供多维度全方位的监控报警服务，包括攻击监控报警、业务可用性监控报警和节点服务质量监控等，保障用户能够第一时间掌握业务应用的各种异常情况。

- **攻击监控报警**

支持以客户为粒度的攻击事件报警，能够实时以客户为粒度监控统计网络层带宽，当发生攻击时，将通过邮件/短信形式向客户报警。

- **业务可用性监控报警**

能够周期性地探测客户业务对应的服务端口，获取应用服务的可用率及延时，如发现应用出现异常情况，将通过短信、邮件等渠道告知相关人员，帮助运营人员第一时间察觉服务异常现象。

◆ **节点服务质量监控报警**

网宿 APP-S 的实时监控报警中心基于监控指标（如 CPU、流量、负载等）对云上各服务节点进行全方位实时监控，一旦出现节点服务异常，将立即向平台运营人员报警，同时平台的智能调度中心自动即时将应用服务调度到正常节点上，保障平台服务稳定可用，避免业务受到影响。

3.2.攻击防御

3.2.1.网络层 DDoS 攻击防御

网络层 DDoS 攻击是攻击者通过伪造大量 IP 地址向目标服务器发起大量数据包，耗尽网络带宽资源进而导致目标服务器无法响应正常的请求。常见的网络层 DDoS 攻击包括 SYN Flood、ACK Flood、ICMP Flood、UDP Flood、各类反射攻击（如 NTP 反射、DNS 反射、SSDP 反射）等。

网宿 APP-S 通过部署智能防火墙，实现对数据报文的实时检测和分析，在不影响正常数据报文访问的前提下，实时高效阻断攻击报文。APP-S 节点防护能力达 600Gbps，平台总体防护能力达 10Tbps+。目前可有效防御 SYN Flood、UDP Flood、ICMP Flood、NTP 反射攻击、SSDP 反射攻击、DNS 反射攻击等各类流量型 DDoS 攻击。各攻击类型简介及防护方法如下：

◆ **SYN Flood**

➢ 攻击简介

攻击者利用工具或者操纵僵尸主机，向目标服务器发起大量的 TCP SYN 报文，当服务器回应 SYN-ACK 报文时，攻击者不再继续回应 ACK 报文，导致服务器上存在大量的 TCP 半连接，服务器的资源会被这些半连接耗尽，无法响应正常的请求。

➢ 防护原理

采用异构防护架构，利用国内独创的专利技术实时检测过滤畸形包（如长度值异常等）和不符合规则的报文，同时通过 SYN Cookie 校验、重传验证等方式完成客户端的协议行为验证，从而在不影响正常客户端连接的情况下阻断攻击。

◆ **ACK Flood**

➢ 攻击简介

攻击者利用工具或者操纵僵尸主机，向目标服务器发送大量的 ACK 报文，服务器忙于回复这些凭空出现的第三次握手报文，导致资源耗尽，无法响应正常的请求。

➢ 防护原理

网宿智能防火墙实时存储连接表信息，通过对接收到的 ACK 报文进行智能校验，判断其是否为合法报文，如不合法，则直接丢弃，进而高效阻断攻击报文，不会对正常访问造成影响。

◆ **ICMP Flood**

➢ 攻击简介

攻击者通过对目标发送大量超大数据包（例如：超过 65535 字节的数据包），给服务器带来较大的负载，影响服务器的正常服务，进而令目标主机瘫痪。

➢ 防护原理

智能防火墙实时统计到达目的 IP 的流量，超过设定阈值则直接丢包。

◆ **UDP Flood**

➢ 攻击简介

由于 UDP 协议都是无连接的协议，不提供可靠性和完整性校验，因此数据传输速率很快，成为攻击者理想的利用对象。UDP Flood 的常见情况是攻击者向目标地址发送大量伪造源 IP 地址的 UDP 报文，消耗网络带宽资源，造成链路拥堵，进而网站服务器拒绝服务。

➢ 防护原理

针对没有 UDP 业务的客户，网宿智能防火墙丢弃所有 UDP 包。对于有 UDP 业务的客户，网宿智能防火墙通过速率限制、UDP 报文匹配等方式防御 UDP Flood。

◆ **反射型 DDoS 攻击**

➢ 攻击简介

反射攻击是基于 UDP 报文的一种 DDoS 攻击形式。攻击者不是直接发起对攻击目标的攻击，而是利用互联网的某些服务开放的服务器（如 NTP 服务器、DNS 服务器），通过伪造被攻击者的地址、向该服务器发送基于 UDP 服务的特殊请求报文，数倍于请求报文的回复的数据被发送到被攻击 IP，从而对后者间接形成 DDoS 攻击。

➢ 防护原理

网宿智能防火墙直接过滤来自常用的反射端口（如 NTP、DNS、SSDP 等）的报文防御反射型 DDoS 攻击。

3.2.2.空连接防御

➢ 攻击简介

攻击者模拟正常用户与服务器建立连接，但是不发送任何数据报文，导致服务器并发连接数高，进而耗尽服务器的处理性能。

➢ 防护原理

网宿 APP-S 通过智能防火墙与客户端请求建联，确认客户端有数据报文发送之后再将连接请求转发至服务器，对于没有发送数据报文的连接请求直接丢弃。

3.2.3.类 CC 攻击防御

➢ 攻击简介

攻击者模拟正常用户与服务器建立连接后，发送大量伪造的数据报文，进而消耗服务器的处理性能和带宽资源。

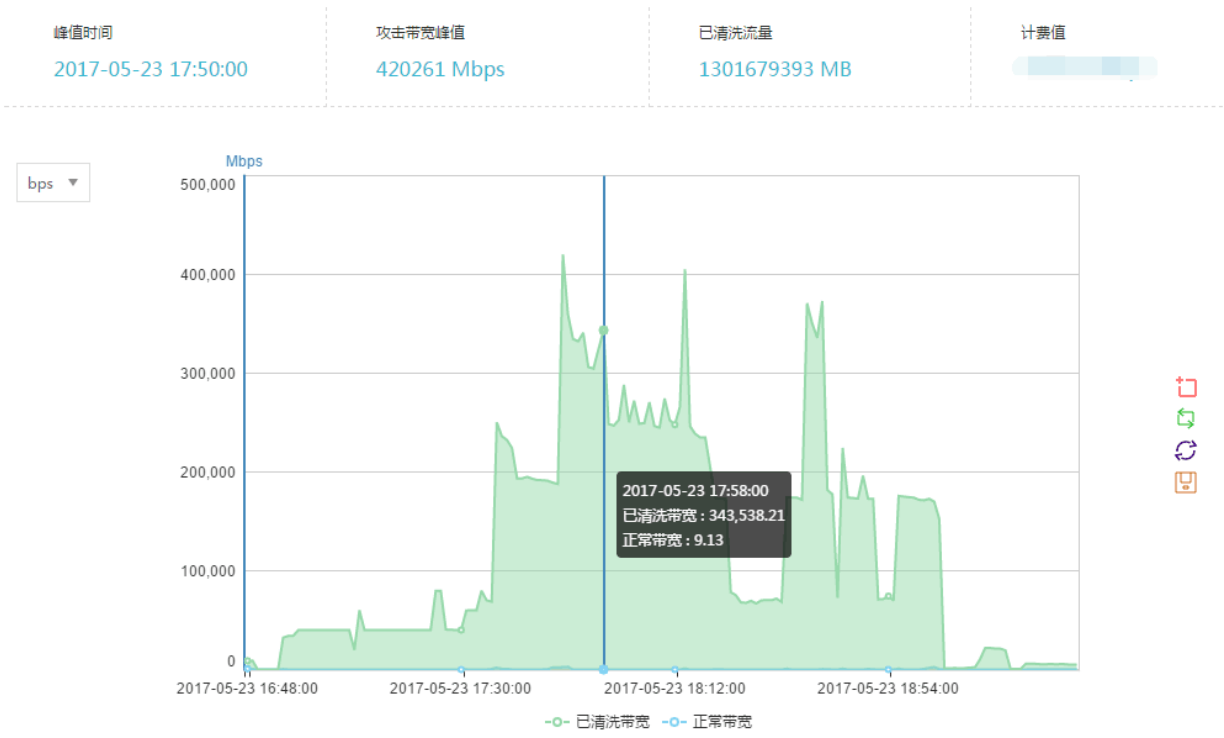
➢ 防护原理

1. 威胁情报库：网宿 APP-S 通过大数据分析平台，实时汇总分析攻击事件的异常 IP，并对这些特征进行威胁等级评估，形成威胁情报库，对于高风险性的 IP 会自动下发到全网防护节点中，一旦后续请求命中高风险 IP，则直接拦截，形成单点攻击，全网联动的防御体系，最大限度地提高防御效率。
2. 速率限制：通过 IP 速率限制，实时分析 IP 和端口的并发连接数，超出阈值的 IP 将直接拦截。
3. 特征包匹配：应用系统大部分是私有的或者不常见的协议，其数据报文格式与客户的应用紧密相关，没有标准规范，导致攻击包的特征千差万别，因此网宿的安全团队将深入分析客户的业务特征，进行数据包特征匹配，进而配置专属的防护方案，有效避免客户业务由于此类攻击造成的影响。

3.3.防护报表展示

网宿 APP-S 能够实时展示 DDoS 防护信息，便于相关人员及时了解整体攻击情况。

1. 能够实时展示客户遭遇攻击的峰值时间、带宽峰值、已清洗攻击流量等，使客户及时了解攻击防护情况。

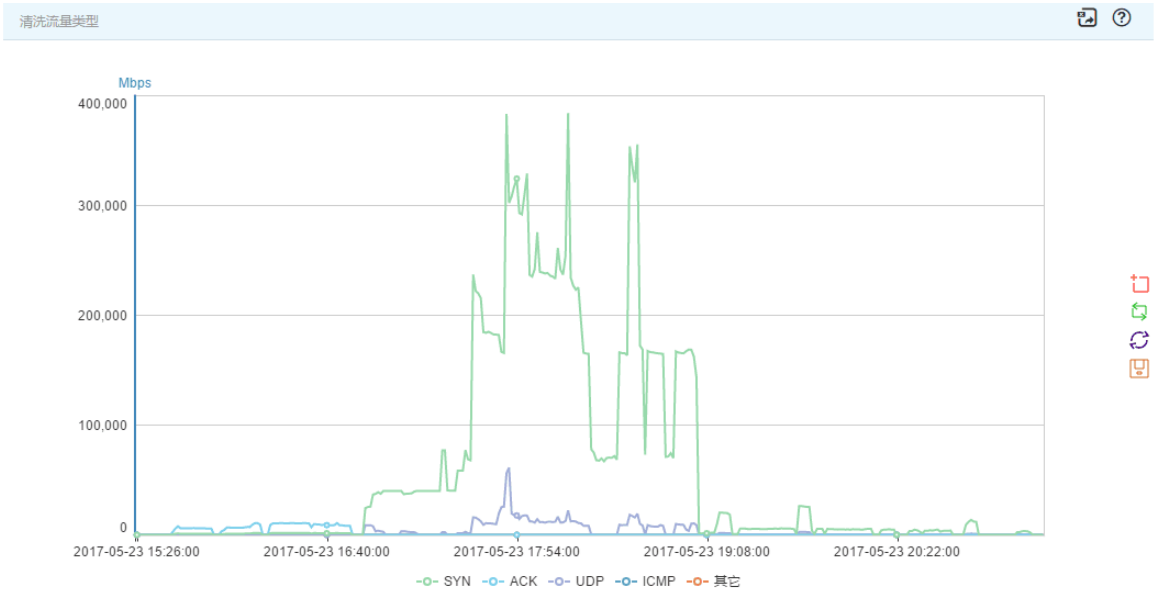


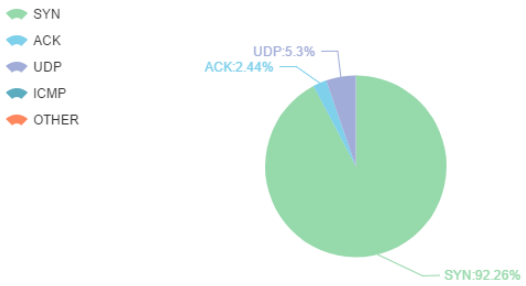
2. 能够实时查看攻击事件，包括攻击开始时间、结束时间及攻击峰值。

攻击事件

序号	攻击开始时间	攻击结束时间	攻击峰值
1	2017-05-23 15:40:00	2017-05-23 22:27:00	420261.36Mbps
2	2017-05-23 23:45:00	2017-05-23 23:45:00	19589.17Mbps

3. 查看攻击的流量类型。





	总流量(G)	百分比
SYN	1,209,383.4	92.26%
ACK	31,940.69	2.44%
UDP	69,469.39	5.30%
ICMP	4.56	<0.01%
OTHER	0	<0.01%
汇总	1,310,798.04	>99.99%

3.4.加速服务

APP-S 由分布在全国各地的各运营商节点组成，通过智能调度，将访问者的请求引导至 APP-S 网络中最佳（距离最近、节点负载最轻）的服务节点，使用户能够就近访问，加快访问速度，提升用户体验。

4. 方案价值

4.1.针对应用业务特点，提供多种接入方式

网宿应用安全解决方案（APP-S）提供多种接入方式（CNAME、HttpDNS、IP 接入），无需改变现有拓扑架构，不需添加任何硬件，客户只需根据自身业务特点选择合适的接入方式，即可享受专业的 DDoS 防护服务。

4.2.紧贴业务特征，有效应对复杂多变的类 CC 攻击

应用系统的数据报文格式与业务应用本身紧密相关，没有标准规范，因此其攻击特征复杂多变，防御难度极大，如采取暴力的直接拦截，将造成误杀，影响业务开展。网宿 APP-S 能够通过信誉库、速率限制等方式防御针对应用系统的 CC 攻击，且网宿的安全团队能够深入分析客户的业务特征，进行数据包特征匹配，进而配置专属的防护方案，有效应对这类攻击，使客户业务避免由于此类攻击造成影响。

4.3.无畏突发大流量 DDoS 攻击

应用系统一旦遭受 DDoS 攻击将严重影响企业业务的正常运作。网宿 APP-S 拥有多个大容量节点，目前单节点抗攻击能力最高可达 600Gbps，同时 APP-S 的智能调度中心能够根据攻击情况智能调度全网资源，总体抗攻击能力达到 10Tbps+，当突发大流量攻击时，APP-S 可以全力保障客户的业务不中断。

4.4.按需防护，降低企业成本

网宿 APP-S 能够根据 DDoS 攻击情况按需提供服务，如遇突发大流量攻击则智能调度全网带宽资源为客户抵御攻击，攻击结束后能够智能调度走多余资源，可以有效避免传统硬件设备“买少了防不住，买多了闲置”的情况。同时也减少了购买安全设备（一台安全设备花费需 5-30 万，平均生命周期 3 年左右）与网络带宽（目前国内二线城市机房 10G 带宽大概是 150 万/年）的费用支出，并减少了聘请专业安全运维团队的人力成本，大幅度降低了企业安全防御的成本。

4.5.高效应急响应能力

鉴于应用系统极易遭受大流量 DDoS 攻击，且攻击特征的复杂多变性，因此突发大流量 DDoS 攻击时服务团队的响应速度直接影响到客户能否度过攻击。网宿 APP-S 提供专属安全服务团队为客户一对一 7*24 小时的贴身服务，突发大规模攻击时能够保障及时响应，提供各项应急预案，保障客户的业务不受影响。

关于网宿

网宿科技 始创于 2000 年 1 月，主要提供互联网内容分发与加速（CDN）、云计算、云安全、全球分布式数据中心(IDC) 等服务。

2009 年 10 月，网宿科技在深交所上市，股票代码 300017。

网宿科技拥有遍布全球的 1000+ CDN 加速节点，在北京、上海、广州、深圳等地设有分公司，在美国、香港、印度、爱尔兰、马来西亚、济南、南京、杭州等地建有多家全资子公司，并在厦门及美国硅谷设立了研发中心。现有员工 3000 多名，研发以及技术人员占总人数 60% 左右。客户群覆盖各类互联网门户网站、视音频网站、网络游戏公司、电子商务网站、政府网站、企业网站以及运营商等，公司服务的客户超过 3000 家，是市场同类公司中拥有客户数量较多、行业覆盖面较广的公司。