方案详述

电子政务专有云

政府行业对数据的使用、传输、存储提出了严格的自主可控要求

- 非常态化上云"的协同防御模式能够满足政府对数据自主可控的合规监管要求
- 一键上云，满足政府行业对产品易用性和运维管理便捷化要求

企业级数据中心与IDC

帮助企业解决敏感数据安全可控、本地业务连续性保障和增值服务场景业务适配的问题

- 云端提供高达400G攻击流量清洗能力，有效保护用户业务连续性
- 本地防护+云端清洗资源联动，满足诸如IDC或具有安全增值服务对外输出场景的需求

其他在线业务

支持面向行业用户和个人用户提供抗DDoS、WAF、DNS解析接入与高防、全网CDN加速与分发服务

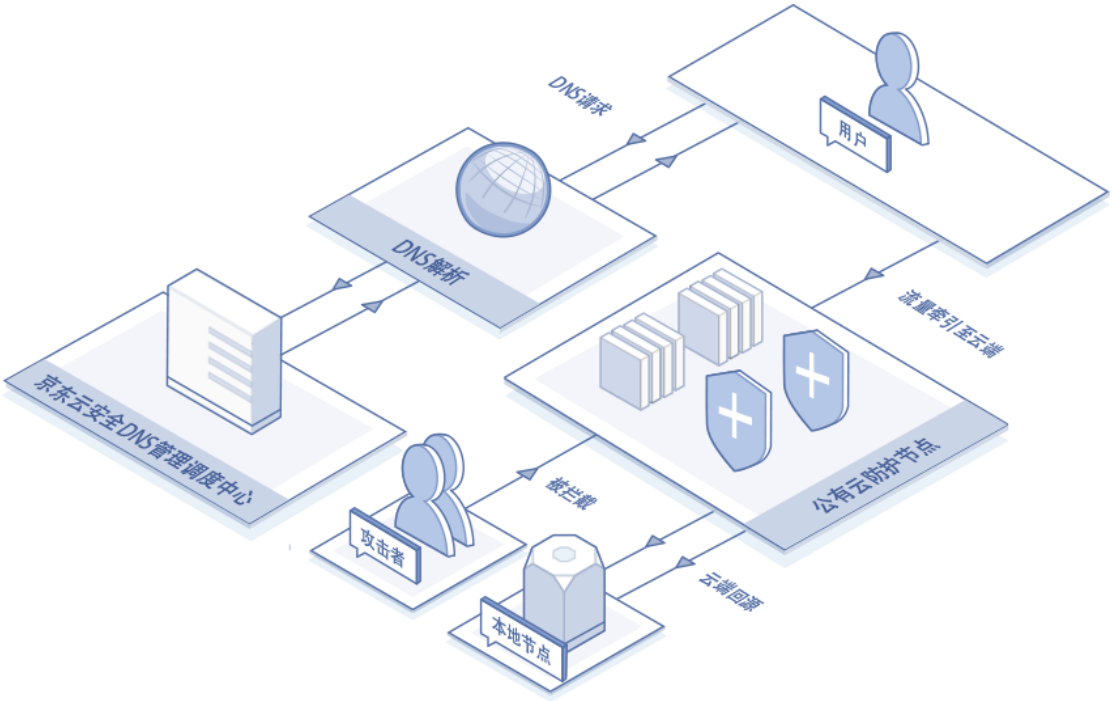
- 企业门户网站
- 网络游戏
- 互联网金融在线交易结算、在线支付
- 网上银行、网上商城

京东公有云业务

使用京东公有云产品和服务的用户可免费使用DDoS基础防护模块，该模块提供 2Gbps防护能力，并支持与京东云IP高防模块、云 WAF 联动，为京东云上的用户业务提供全面的防护能力

- 京东云上构建的网站、数据库、存储系统
- 京东云上构建的企业门户、支付、结算和交易系统
- 京东云上构建的企业电商平台、业务总线、注册与订阅接口服务

方案架构

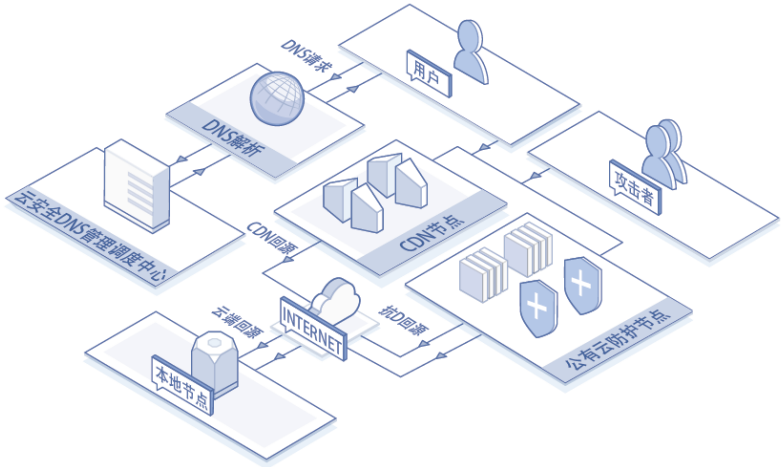


架构说明

100Gbps DNS 防护能力 CNAME、NS 接入 单点防御能力超过 400Gbps 本地防护+一键上云 准确识别和拦截流量泛洪、畸形报文、伪造请求、慢速连接、CC 攻击等 高效防御 SQL 注入、XSS 跨站脚本、恶意路径穿越、网页挂马、网页篡改等

典型场景

融合防御模型



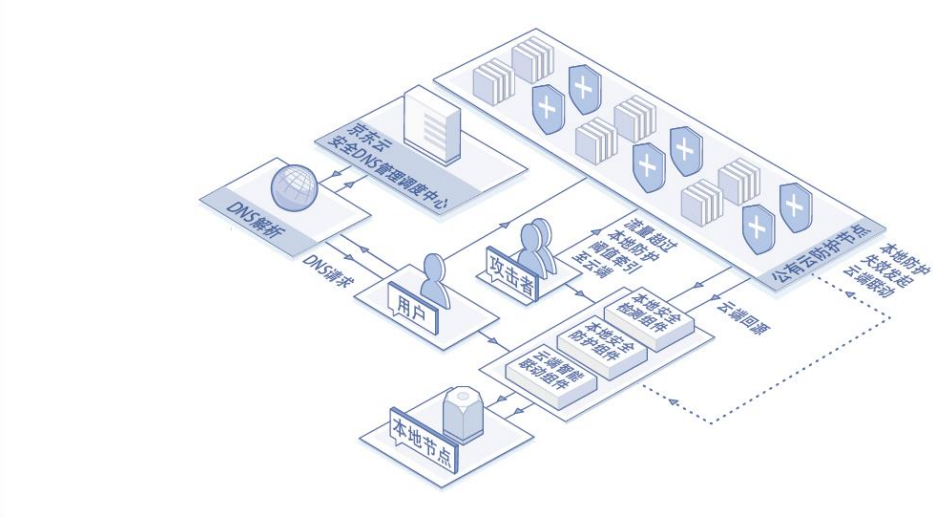
典型场景： 客户使用 CDN 加速场景下，缺乏抗 DDoS 防护能力，但单纯串联 IP 高防+CDN

又无法起到加速效果。

解决方案： 为用户源站内容提供静态本地加速和动态优化回源加速服务，进一步提升用户访问体验，全网任一 CDN 加速节点如遭遇大规模 DDoS 攻击，可实时与网内的抗 D 节点联动，实现攻击流量牵引和正常回源，确保用户业务的连续性不受 DDoS 攻击影响。攻击缓解或停止后，可动态调度到最优的 CDN 节点，保护用户体验，可实现全程用户无感知。

使用产品： IP 高防 CDN 云解析 DNS

联动防御模型

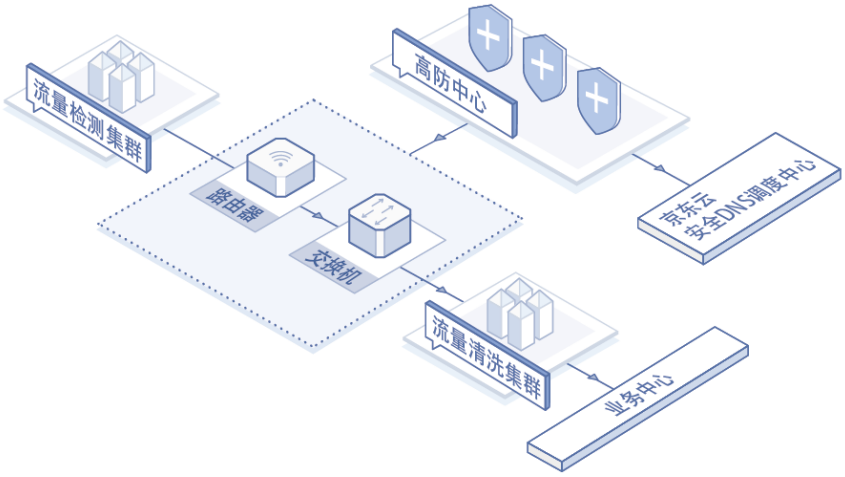


典型场景： 企业本地 IDC 机房缺乏安全防护措施，本地业务和网站易遭受 SQL 注入，XSS 跨站等应用层攻击，单独部署硬件防护设备又无法抵御海量 DDoS 攻击

解决方案： 为企业本地机房部署安全检测和防护组件，提供基础安全防护能力，当本地遭遇大规模流量攻击时，可通过一键上云功能将流量牵引至云端，确保 DDoS 攻击不会对本地出口带宽和其它业务造成任何影响，并使被攻击业务持续可用

使用产品： IP 高防 Web 应用防火墙云解析 DNS

本地在线部署模式

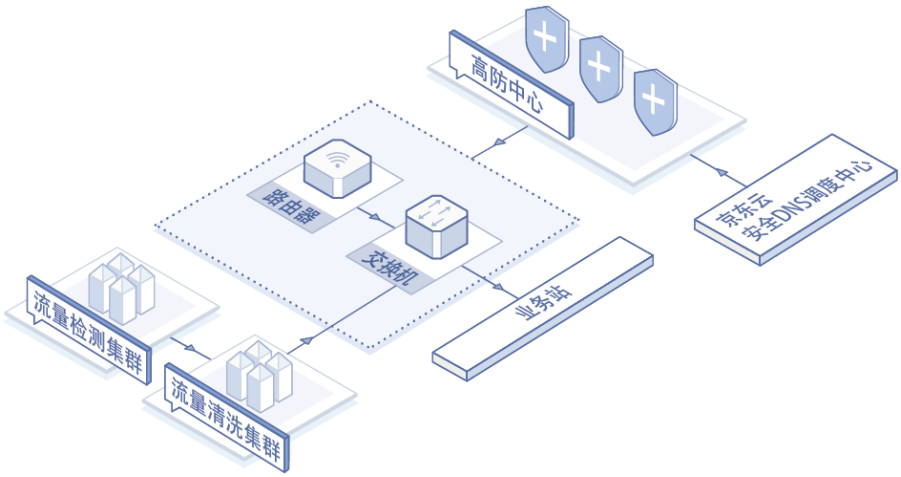


典型场景： 1.流量被转发到清洗集群，处理完成后再被转发到 WAF/Cache 集群 2.WAF/Cache 集群将安全的流量转发到源站 3.当流量检测集群发现大流量攻击时即开启云端联动模式 4.云端 DNS 调度中心将流量牵引至云端高防中心 5.高防中心将过滤后的纯净流量转发到原有网络

解决方案： 流量检测集群采用旁路部署，接入流量镜像即可；流量清洗集群和 Waf/Cache 集群支持旁路 BGP 模式，提升容错性；可按需牵引，确保业务高可用，有效保护用户体验；支持自动应急上云和人工一键上云，配置灵活，解放运维人员

使用产品： IP 高防 Web 应用防火墙域名服务

本地旁路部署模式



典型场景： 1.在没有被攻击时，流量被转发到业务站 2.当流量检测集群发现时即通知清洗集群进行 BGP 迁移（32 位掩码的精细路由，清洗集群成为去往被攻击目标流量下一跳） 3.流量清洗集群支持将纯净流量注入到原有网络中 4.当流量检测集群发现大量流量攻击时即开启云端联动模式 5.云端 DNS 调度中心将流量牵引至云端高防中心 6.高防中心将过滤后的纯净流量转发到原有网络

解决方案： 流量检测集群采用旁路部署，接入流量镜像即可；流量回注可支持策略路由回注和三层回注两种方式；可按需牵引，确保业务高可用，有效保护用户体验；支持自动应急上云和人工一键上云，配置灵活，解放运维人员

使用产品： IP 高防 Web 应用防火墙云解析 DNS

优势

全场景适配能力

基于对多个行业的业务场景深度理解，能够全面适应和满足政府、金融、IDC、游戏、电商、互联网等多类业务场景的安全防护和内容加速需求，可提供丰富的产品形态和 API 接口，满足不同行业在安全合规、运维管理、业务开发等多方面业务需求。

合规与监管遵从

本地组件提供攻击检测和防护能力，一般情况下请求和应答的数据无需经过云端节点，仅当攻击流量过大时才进行迁移，这种"非常态化上云"的协同防御模式能够满足政府、金融行业的数据自主可控的合规监管要求。

智能化纵深防御

横向提供从网络边界延伸至主机层的最大防御纵深，纵向拉通和联动用户本地防护组件和云端资源： •基于京东云智能调度指挥系统，可使抗D与CDN智能联动，最大限度保证加速效果； •整合云端态势感知与威胁情报，积极响应和预测业务安全趋势，为分析与决策提供数据参考与支持； •整合攻击事件/网络痕迹大数据与攻击者行为画像，帮助用户建立业务置信曲线，降低误报和漏报

接口与数据开放

可提供结构化原始防护日志数据供用户参考，帮助用户更高效的完成安全事件响应和分析，同时还可以提供丰富的 API 接口，为增值安全服务输出场景提供支持。

动态的优化调度

抗 D、WAF、CDN 等功能模块能够实现无缝融合与联动，支持根据用户实际业务场景实现智能化动态调度，完美解决传统 CDN 抗 D 模式导致的全局加速效果被破坏的问题，为用户规划最优的转发与回源路线，支持跨运营商多线路，降低延迟，进一步提升用户体验，可实现用户业务被攻击时无感知的调度与保护。

深厚的经验积累

基于十几年来的安全研究、安全产品开发与行业安全最佳实践，备受京东商城、京东金融、京东保险的青睐，为618、11.11、12.12 大促提供全程保障，并为多地政府及电子政务云提供全程防护支持，助力十八/十九大、两会、一带一路、金砖五国会议重保期间的安全保障工作。多年来持续得到市场的检验与认可，在多个行业获得了丰富的成功案例，积累了大量的实践经验，对不同行业的业务场景和客户痛点具有深入的理解，可提供业务场景级的产品和解决方案，帮助用户解决业务场景内的安全问题，提升客户业务竞争力。

推荐产品

Web 应用防火墙

针对网站业务流量进行恶意特征识别及防护，避免网站服务器被恶意入侵，保障业务的核心数据安全。

¥500.00/月

IP 高防

针对遭受大流量的DDoS攻击的用户提供增值防护的服务。通过将业务IP替换成高防IP的方式，隐藏源站。

¥6000.00/月

CDN

基于京东优质网络基础设施和智能云计算技术，向客户提供低成本、高性能、可扩展的互联网内容分发服务。

CDN流量10GB内，¥0.35元/GB