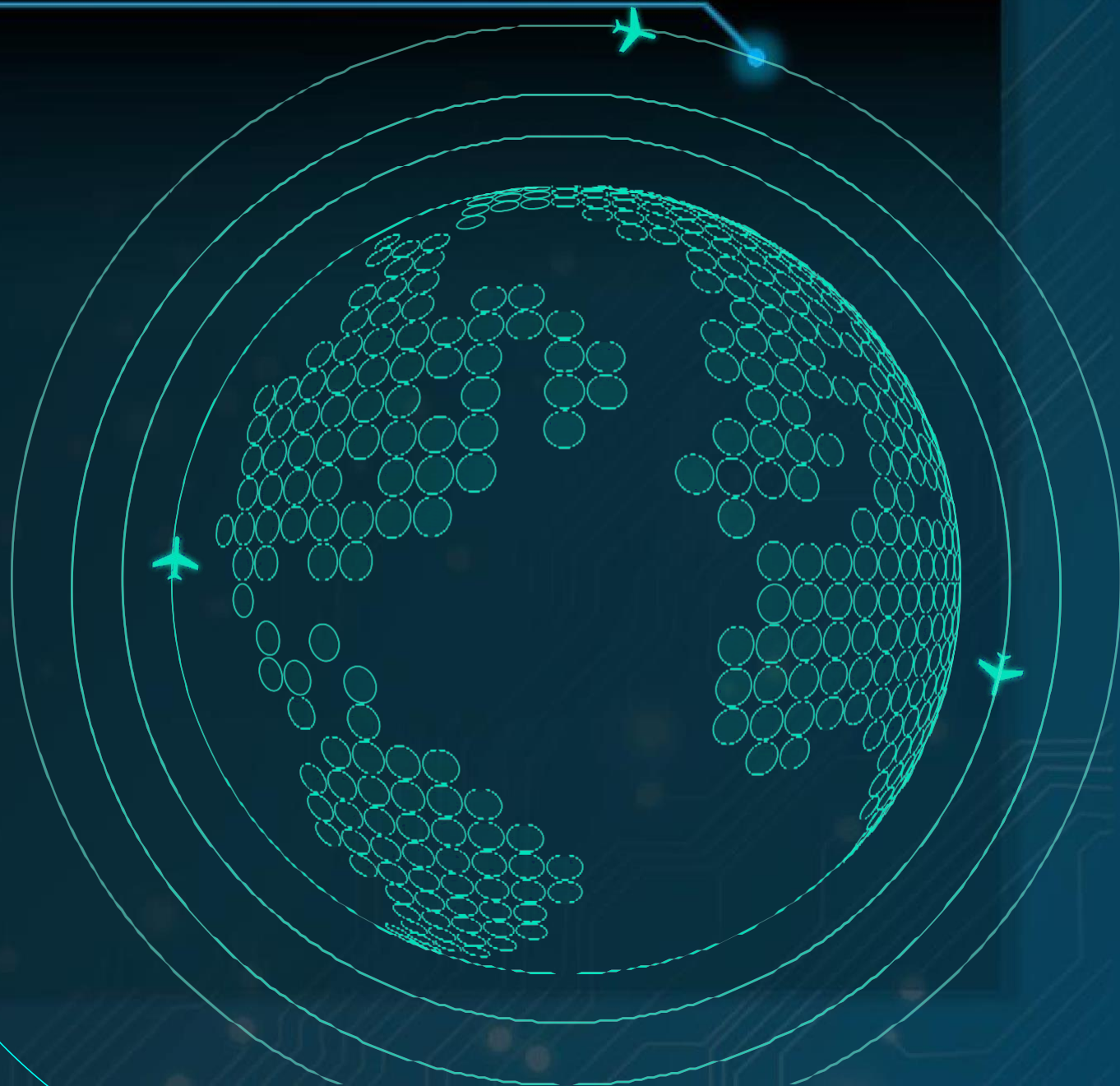
网站安全防护云平台

GOODWAF



网站安全现状

学习通数据库泄露

超星学习通是国内众多高校使用的电子化课程学习软件。2022年6月，有公众号博主发现社工库正在🎧售超星学习通数据库，这份数据库包含1亿7273万条数据，同时还包含1076万条密码，数据涉及学校名称、学生姓名、注册手机号码、学号、工号、性别以及邮箱等。

软件勒索

1月21日，我国台湾地区电子产品制造公司台达电子（Delta Electronics）发布声明称，其受到一起勒索软件攻击，与Conti勒索软件团伙有关。当地媒体报道，有记者已获得一份内部事件报告副本，报告数据显示这次攻击实际情形非常严峻——台达电子1500多台服务器和12000多台计算机已被攻击者加密。据称，攻击者向这家台湾电子产品制造商索要1500万美元的赎金。

Apache Log4j2高危JNDI注入漏洞

2021年11月24日，阿里云安全团队向Apache官方报告了Apache Log4j2远程代码执行漏洞。ApacheLog4j2是一个用于Java的日志记录库，其支持启动远程日志服务器。由于Apache Log4j2某些功能存在递归解析功能，攻击者可直接构造恶意请求，触发远程代码执行漏洞。

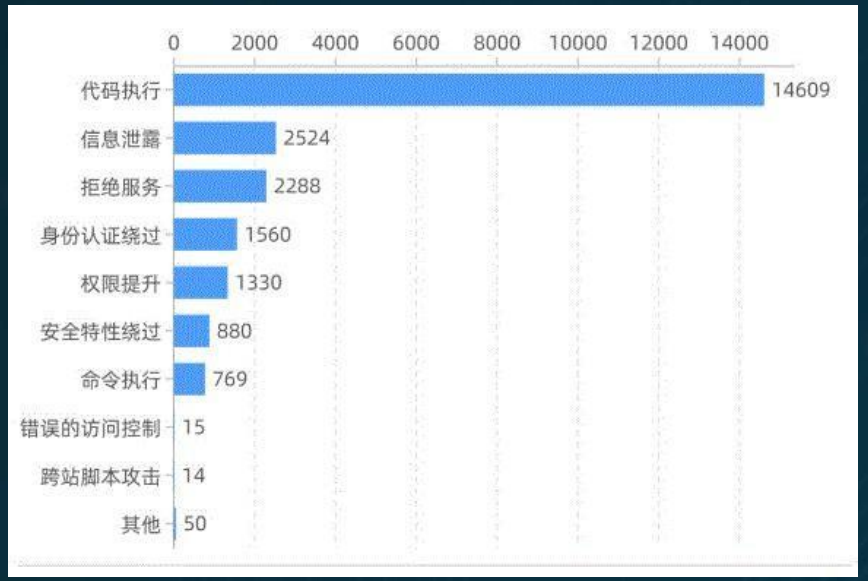
QQ大规模被盗号

2022年6月26日晚间，标题为“QQ盗号”“QQ回应大批账号被盗”的词条相继登上微博热搜，大量QQ用户反映，自己的QQ账号被盗。27日上午，腾讯QQ官方微博发文回应称，其自6月26日晚10时左右收到部分用户反馈的QQ账号被盗一事，经调查发现主要原因系用户扫描过不法分子伪造的游戏登录二维码并授权登录，该登录行为被黑产团伙劫持并记录，随后被不法分子利用发送不良图片广告。

网络攻击数量愈发增 加

2022年度新增漏洞近2.5完个，达到历史新高，保持连年增长态势。超高危级漏洞占比呈持续上升趋势，漏洞修复率大幅提升，面临漏洞威胁形势依然严峻。

以代码执行漏洞、信息泄露、拒绝服务为主要漏洞类型。



网站安全政策&法规

行业	政策	解读
政府	1、2015年9月，四部委联合发文关于印发《党政机关、事业单位和国有企 2、2015年3月《国务院办公厅关于开展第一次全国政府网站普查的通知》	1、对政府网站的可用性、敏感内容等方面提出了要求。
金融	1.中国银监会办公厅关于银行业金融机构互联网网站安全专项整治行动有关事项的通知（银监办发〔2015〕169号）	1、要求需加强网站的安全监测和检查，积极查找网站安全隐患并及时整改。
	2.证监会颁布的《证券公司网上证券信息系统技术指引》、中国人民银行颁布的《银办函［2009］646号》文件。	2、对银行、证券、基金公司的网站提到了严格的要求。
	3.其他相关文件：《关于防范网银诈骗加强安全技术防范措施的通知》《关于银行业金融机构互联网网站安全专项整治行动有关事项的通知》《商业银行监管评级达标指南》	3、相关内容要求应对对外开放web的应用系统进行木马、钓鱼、web漏洞、页面篡改、敏感内容、性能检测等情况进行监控。
公安	1、2018年11月《公安机关互联网安全监督检查规定》开始实施施行	1、互联网服务提供者和联网使用单位是否存在网络安全漏洞，可以开展远程检测
税务	1.从2016年开始税务总局会对省级税务进行网络安全相关指标的绩效考核	1、考核范围涉及包括网站漏洞、网站可用性、失效链接等进行检查。
教育	1.2017年5月教育部印发了关于《教育行业网络安全综合治理行动方案》的通知。	1、提出四项工作内容。第一，治理网站乱象，强化主体责任；第二，堵塞安全漏洞，增强防护能力；第三，补齐等保短板，履行安全保护义务；第四，规范安全管理，提升治理水平。
其他	1.中央网信办、工业和信息化部、公安部、市场监管总局四部门于2019年5月至2019年12月，联合开展全国范围的互联网网站安全专项整治工作	其中对落实网络安全义务不到位，发生网页篡改、被植入后门木马等网络安全事件，依据情节严重程度，采取约谈主要负责人、停业整顿、关闭网站、注销备案等措施并公开曝光，涉企行政处罚信息将依法纳入市场监管总局国家企业信用信息公示系统予以公示。

政府

等保、法规

- 等保2.0在1.0的基础上，更加注重全方位主动防御、动态防御、整体防控和精准防护。
- 等保2.0充分体现了“一个中心三重防御“的思想，一个中心指“安全管理中心”，三重防御指“安全计算环境、安全区域边界、安全网络通信”，同时等保2.0强化可信计算安全技术要求的使用。

集约化

- 国务院办公厅关于印发《政府网站集约化试点工作方案》的通国办函〔2018〕71号
- 实现基础设施集约、应用支撑平台集约、服务集约。

政务云

- 面向政府行业，由政府主导，建设运营的综合服务平台，一方面可以避免重复建设，节约建设资金，另一方面通过统一标准有效促进政府各部门之间的互连互通、业务协同，避免产生“信息孤岛”，同时有利于推动政府大数据开发与利用，是大众创业、万众创新的基础支撑。

企业

1

本地安全运维

- 本地化安全运维团队，受制于技术实力、资金投入
- 安全风险、0day漏洞随时爆发，本地更新时效性无法保障

2

安全要求

- 国家、监管部门安全要求
- 用户数据隐私，关键技术保护
- 公司声誉、品牌形象，与安全事件息息相关

3

数据分析

- 用户群里、用户所在区域、兴趣内容板块等用户资源大数据分析
- 业务高峰态势、资源扩容参考、运营成本核算、项目投入产比

安全痛点

安全监测

业务自查、自审、自测，风险规避

安全运维

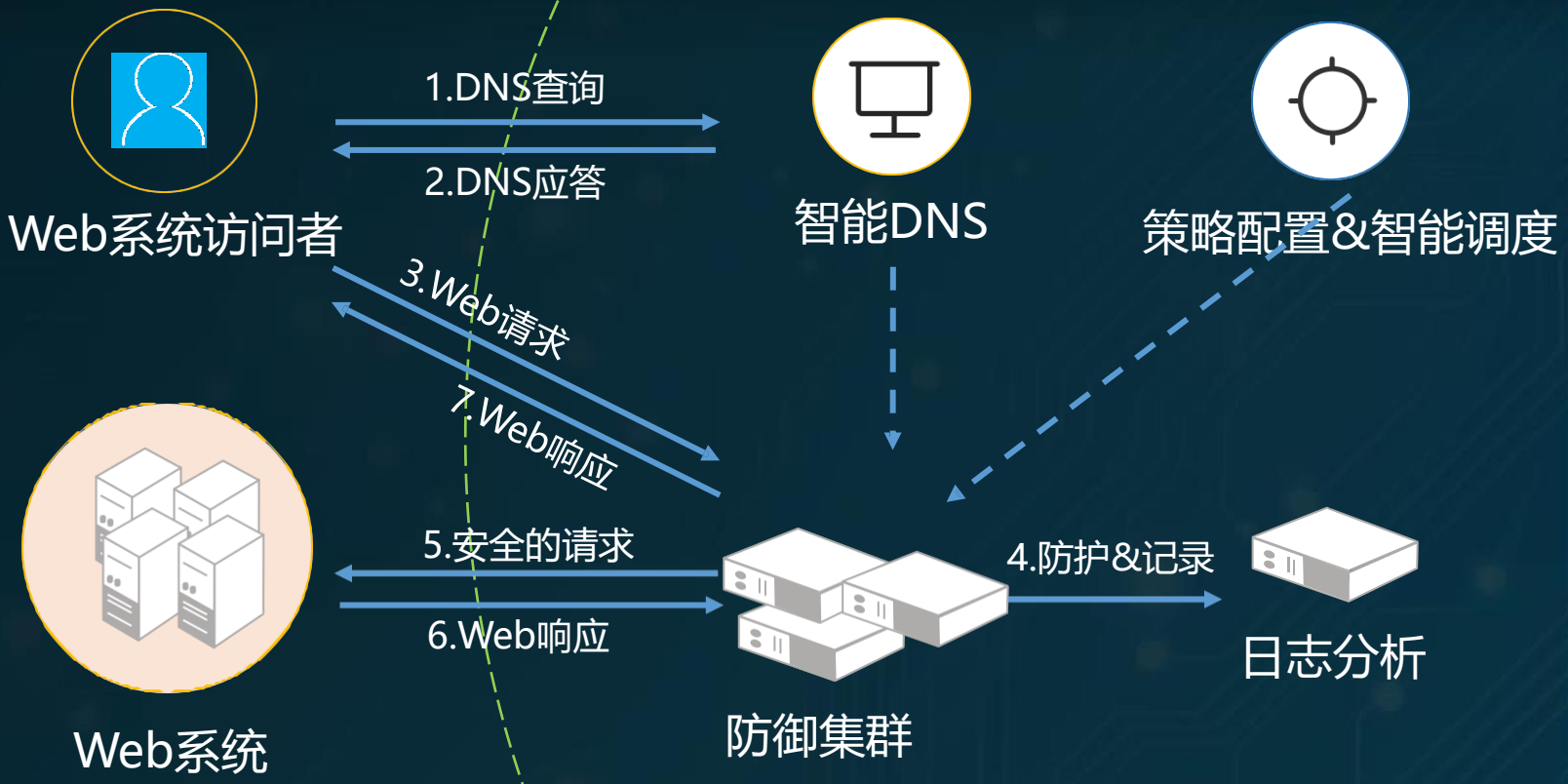
业务更新、迭代、升级，风险可控

安全管理

业务分析、记录、存档，风险取证

产品如何使用

只需将网站的DNS解析到云防护防御节点



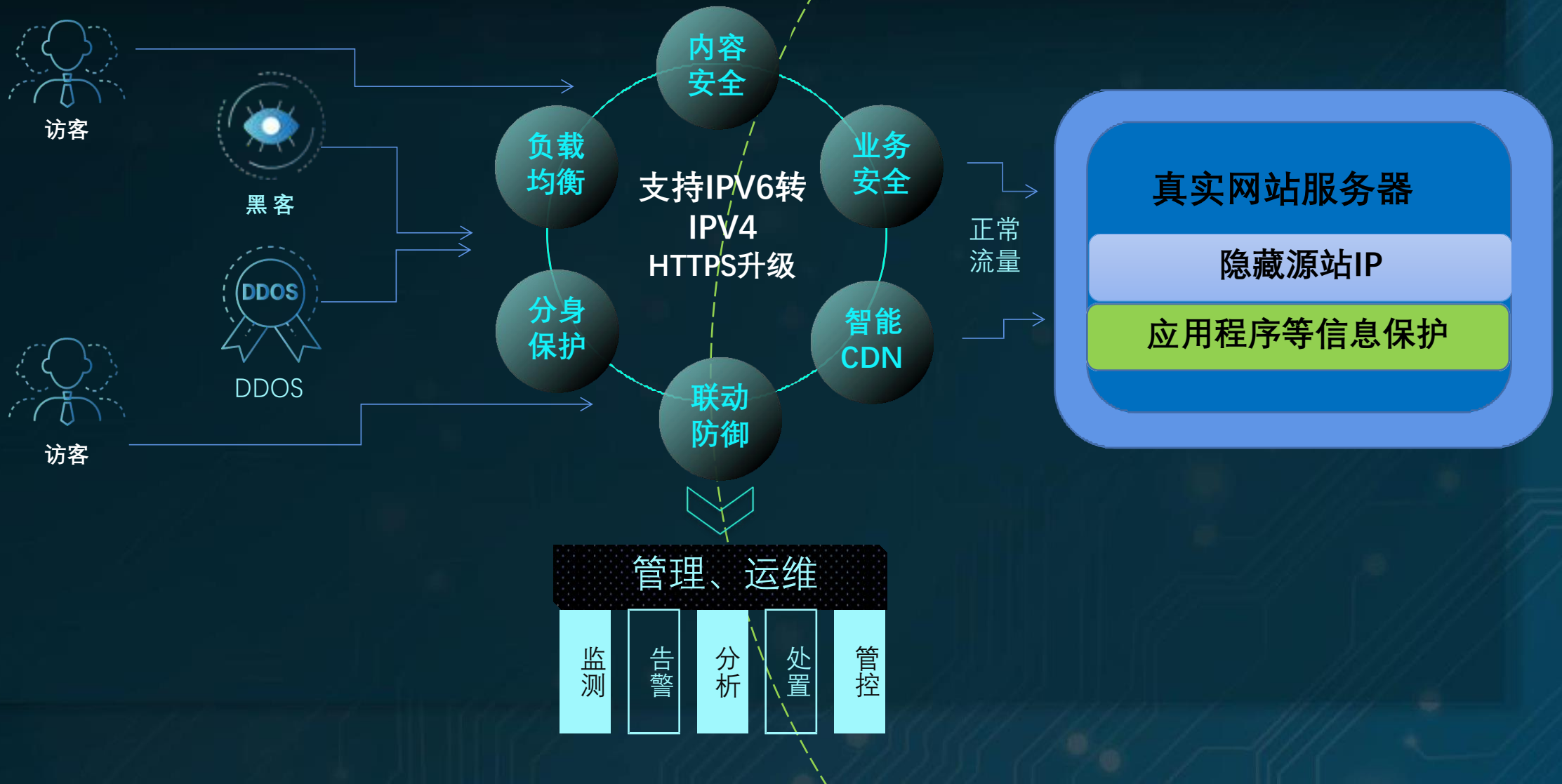
防御流程-防护前

网站安全风险

1. 源站IP、端口暴露公网，端口扫描、恶意攻击风险
2. **网站绩效评估**，源站不稳定时可用性、完整度无法保证
3. 本地资源有限，高峰期访问速度、远距离传输体验无法保障
4. 本地安全设备众多，**防护策略离线更新**不及时
5. 多安全设备无集中管理平台，安全规则、IP封堵、端口开放操作繁琐
6. 网站被攻破、篡改、挂马等造成信息泄露
7. 部分应用存在底层OS、库依赖，🎧现漏洞无法立即更 新到安全版本
8. **0day漏洞威胁**
9. **IPV6支撑改造**，设备投入和改造成本不可预计
10. **HTTP升级HTTPS**周期不可控，数据截取风险突增
11. NAT后应用程序访问日志记录内网IP，无法有效进行大数据统计分析

……

防御流程-防护后


访客
黑客
DDOS
DDOS
访客
内容安全
负载均衡
业务安全
支持IPV6转IPV4
HTTPS升级
分身保护
智能CDN
联动防御
正常流量
真实网站服务器
隐藏源站IP
应用程序等信息保护
管理、运维
监测
告警
分析
处置
管控

产品介绍

01 云WAF

拦截常见的OWASP攻击、分身访问控制、高级云WAF

02 ipv6升级改造

自有ipv6节点，接入后可实现ipv6功能，实现ipv6改造

03 CDN加速

缓存加速内容传输，多线、BGP节点覆盖
全网运营商，HTTP/HTTPS加密传输

04 业务安全

防刷、反爬虫、登录注册保护、防恶意
订单、防活动作弊、防刷库撞库

05 监测、告警

多链路可用性监测
多维度安全检测
安全威胁实时告警

06 态势感知

高级威胁分析，黑客行为追溯，原始
日志下载，攻防态势实时展示。

07 专业服务

技术专家提供7x8小时服务。

08 零部署

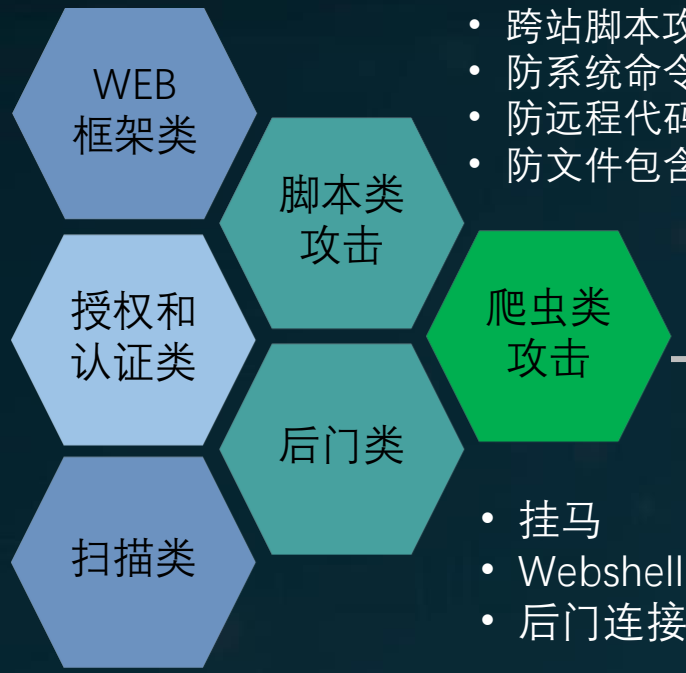
智能DNS实现云防护，源站架构零改动，
可合作运营、可私有化。

云WAF

- 第三方开源软件漏洞

- 注入攻击
- 跨站脚本攻击（XSS）
- 防系统命令执行
- 防远程代码执行
- 防文件包含攻击

- 目录遍历
- 强制浏览
- 跨站脚本请求伪造
- 敏感信息泄漏
- 文件上传



- 挂马
- Webshell
- 后门连接

- 防网站恶意扫描

正常访客

云WAF

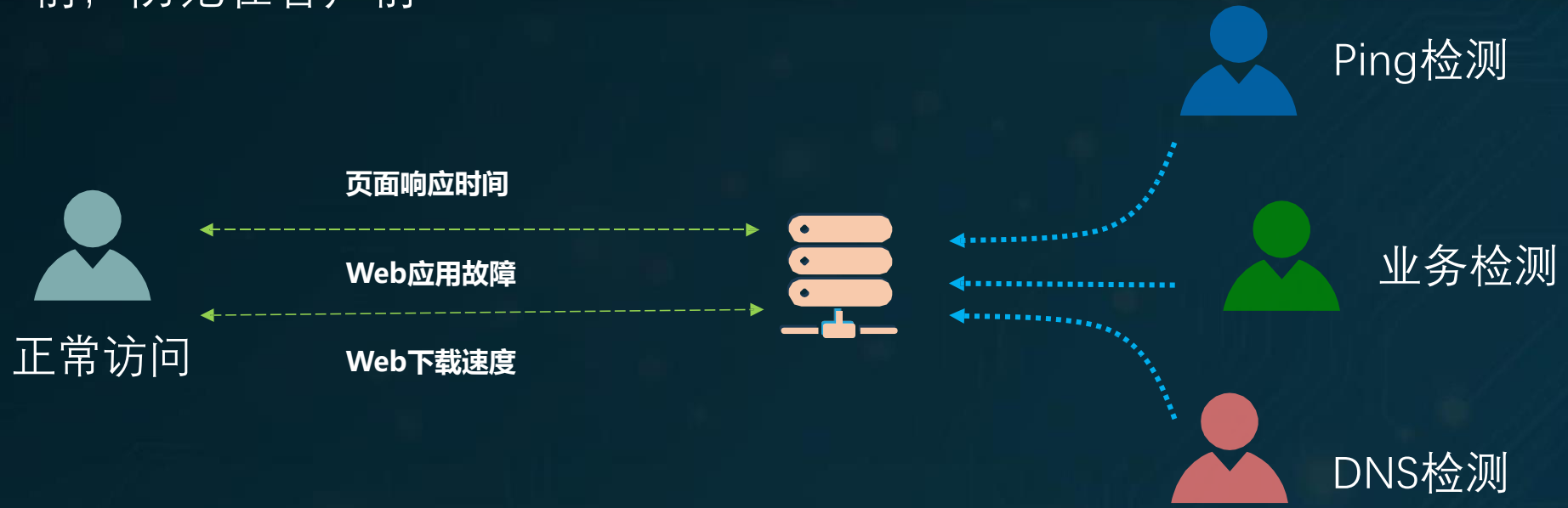
防护网站

CDN加速

将静态内容放入内存，加速动态内容加载速度，
并让您轻松的将输🎧内容最佳化。

业务监测

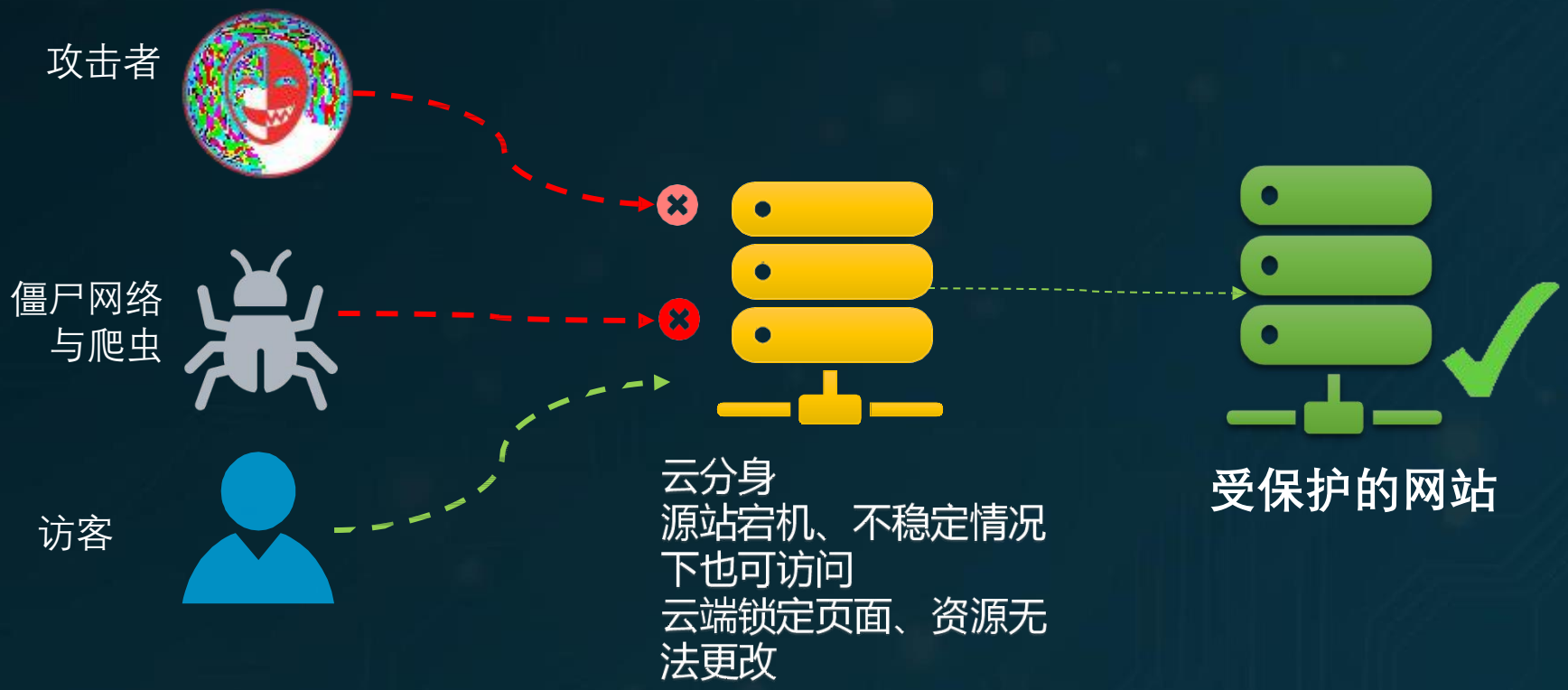
利用自身的云检测系统，时刻想在客户前，
发现在客户前，防范在客户前



云监控:
7x24小时不间断监控
多维度监控网站可用性、性能
网络层面提前预警

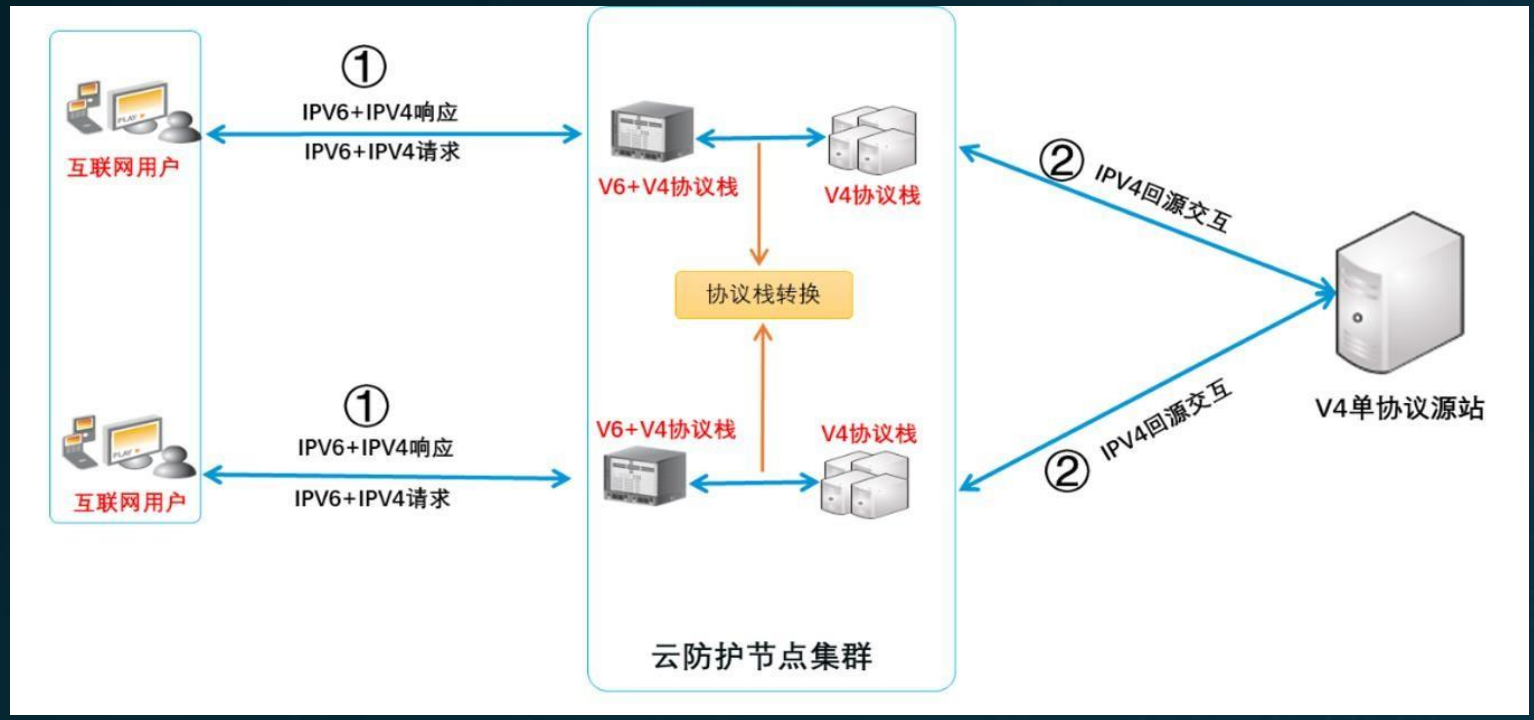
云分身

让您的网站在敏感时期
哪怕源站关闭的情况下也可以对外提供服务

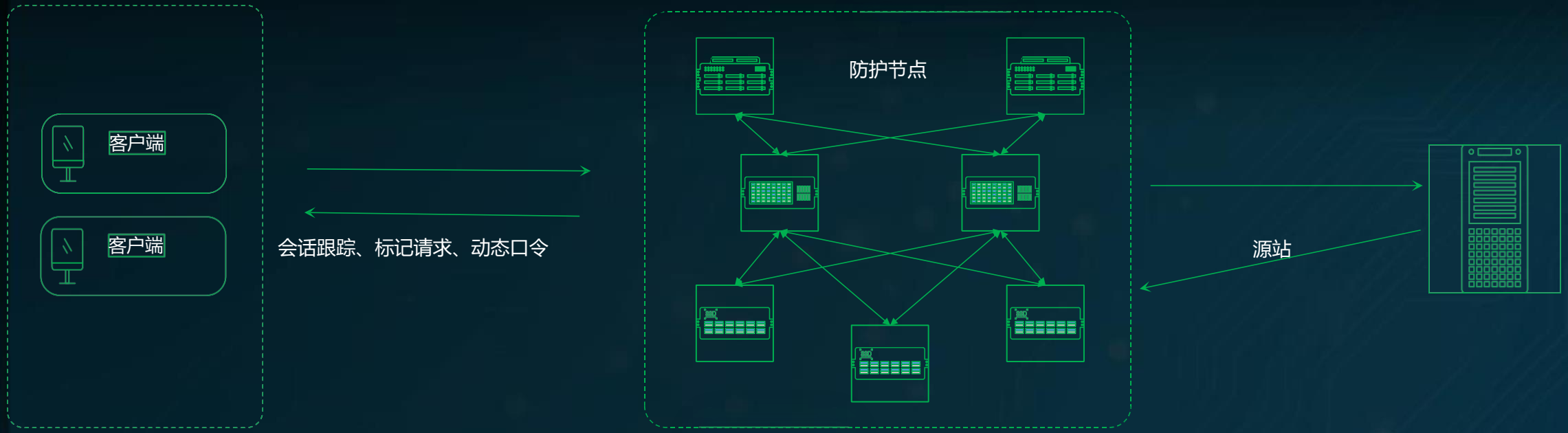


支持IPv6和IPv4双协议栈

帮助网站应用在已有支持IPv4用户访问的基础上,快速支持IPv6访客需求,网站无需进行任何改造,不用添加任何硬件设备。帮助用户一键式、快速完成网站的IPv6访问升级、安全防护的双重难题。



Bot防护



客户端验证

通过对客户端与服务器的动态双向验证，检查运行环境、设备指纹等因素。每次验证都会随机选取检测的项目与数量，增加不可预测性，大幅提高攻击成本。
运行环境监测

动态令牌

动态令牌(Token)是指应用防护系统为用户端可以合法访问的请求分配的一次性“识别码”。用户端每个请求附带的令牌都需要通过服务器端的校验，从而防止违规访问等恶意行为。

优势

让您只需要更改DNS就能保护您的WEB资产，并提高可用性。

在您的服务器受到分布式攻击或其他Web攻击之前我们将其拦截。

基础设施资源

强大而丰富的基础设施资源，自有4.5万平数据中心，提供完善底层服务。

联动防御IP行为分析

基于大数据IP联动防御对访客行为进行分析，智能识别多种黑客攻击，零误封，秒防御，

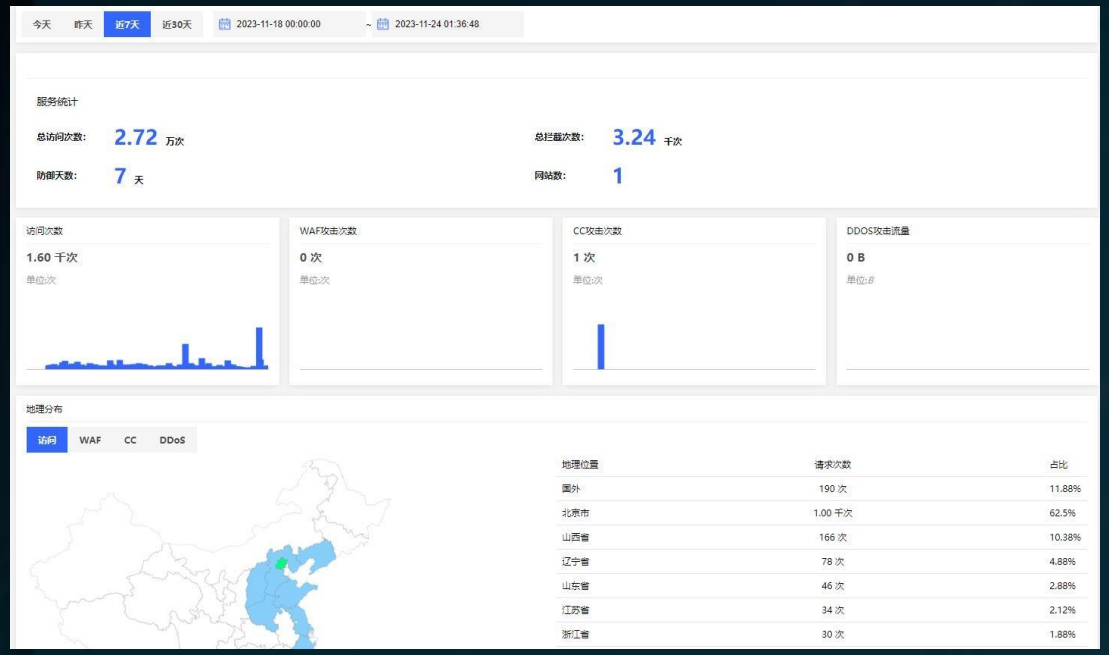
云分身备份功能

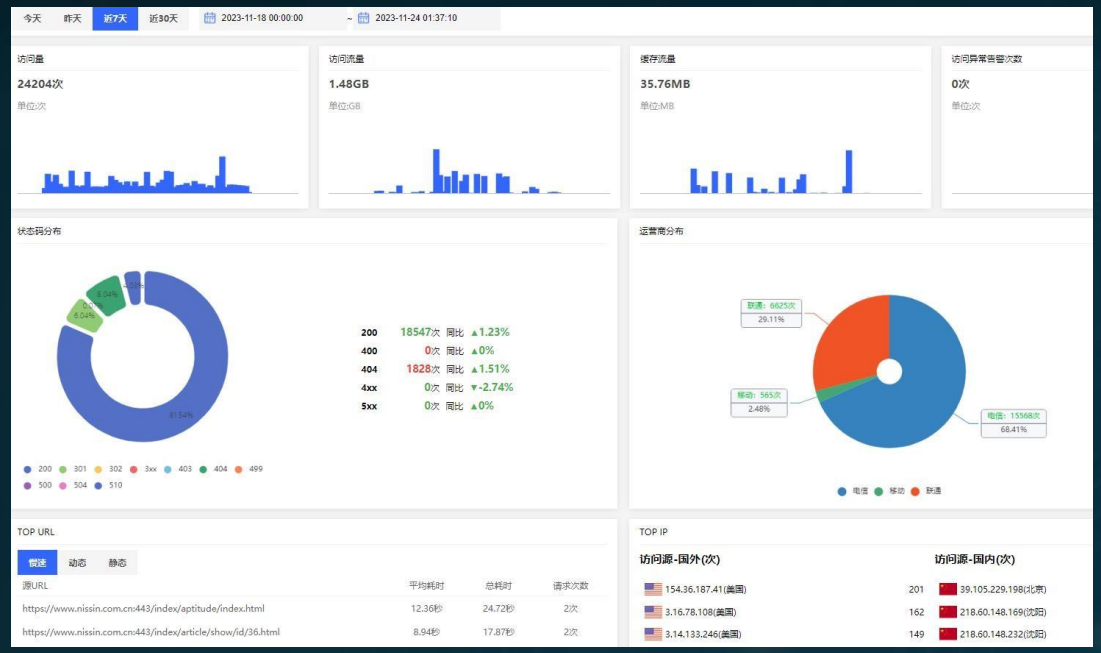
云分身备份恢复功能，保障网站永不宕机

安全态势可视化

网站实时连接详情，日志，全网大数据安全态势可视化。

安全态势可视化


今天 昨天 近7天 近30天 2023-11-18 00:00:00 ~ 2023-11-24 01:36:48
服务统计
总访问次数: 2.72 万次
总拦截次数: 3.24 千次
防御天数: 7 天
网站数: 1
访问次数
1.60 千次
单位:次
WAF攻击次数
0 次
单位:次
CC攻击次数
1 次
单位:次
DDOS攻击流量
0 B
单位:B
地理分布
访问 WAF CC DDoS
地理位置 请求次数 占比
国外 190 次 11.88%
北京市 1.00 千次 62.5%
山西省 166 次 10.38%
辽宁省 78 次 4.88%
山东省 46 次 2.88%
江苏省 34 次 2.12%
浙江省 30 次 1.88%


今天 昨天 近7天 近30天 2023-11-18 00:00:00 ~ 2023-11-24 01:37:10
访问量
24204次
单位:次
访问流量
1.48GB
单位:GB
缓存流量
35.76MB
单位:MB
访问异常告警次数
0次
单位:次
状态码分布
200 18547次 同比 ▲1.23%
400 0次 同比 ▲0%
404 1828次 同比 ▲1.51%
4xx 0次 同比 ▼-2.74%
5xx 0次 同比 ▲0%
运营商分布
联通: 6625次 29.11%
移动: 565次 2.48%
电信: 15568次 68.41%
TOP URL
智速 动态 静态
源URL 平均耗时 总耗时 请求次数
https://www.nissin.com.cn:443/index/aptitude/index.html 12.36秒 24.72秒 2次
https://www.nissin.com.cn:443/index/article/show/id/36.html 8.94秒 17.87秒 2次
TOP IP
访问源-国外(次)
154.36.187.41(美国)
3.16.78.108(美国)
3.14.133.246(美国)
访问源-国内(次)
201 39.105.229.198(北京)
162 218.60.148.169(沈阳)
149 218.60.148.232(沈阳)

业务对象

防护对象

- 网站群体，必须以**域名**为防护· 粒度（IP类网站不 可以）
- 必须使用**HTTP/HTTPS**协议（mail类协议不可以）

客户群体

- 适用于“政府、企业、银行、· 金融、游戏、教育、互联网”等所有涉及WEB应用的各个行业

防护功能

- WEB网站安全防护云平台：WEB攻击防护；业务、内容安全；**IPV6/HTTPS升级**
- 智能CDN加速；态势感知；监测告警；专家服务支撑

本地安全与GOODWAF云防护

	本地安全硬件	GOODWAF
配置复杂度	高	低
大流量攻击	弱（受带宽限制）	强
应用层攻击	强	强
成本（相同性能下）	高	中

云防护与本地安全硬件产品互为补充！