HUAWEI

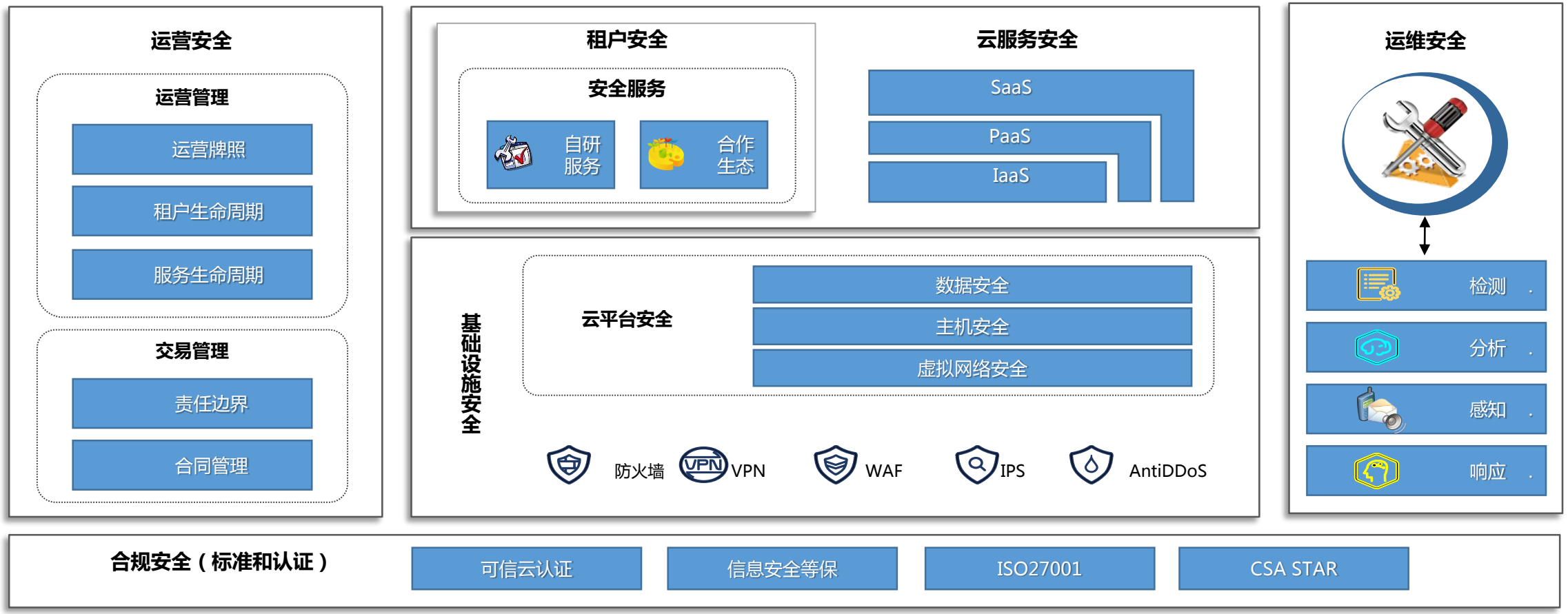
使用安全服务构建安全防护体系

华为云安全架构师 何伟

LEADING NEW ICT

目录

华为云理解中的云安全



以云安全能力为基石，以法律、法规遵从为城墙，以生态合作伙伴为护城河的立体安全体系

安全组网图总览

解决方案安全能力

纵深边界安全防护：

免费5G以下DDOS攻击防御能力 + 200G能力专业高防DDOS服务；
vNGWF、vIDS，华为多年专业技术积累，安全可靠；
高性能、高可用云WAF，支持多种解码能力，检测率高，误报率低。辅以WebScan，达成“先敌发现，积极防御”。

全面主机/应用安全防护：

华为自研HIDS/WTP/ARS/HVD等服务，提供全面的主机侧、应用层安全防护，保障业务安全。

全方位网络隔离与访问控制：

VPC实现各安全域基础隔离，SG实现各VPC基础访问控制，vNGFW实现基于策略的访问控制及AV/IPS等。

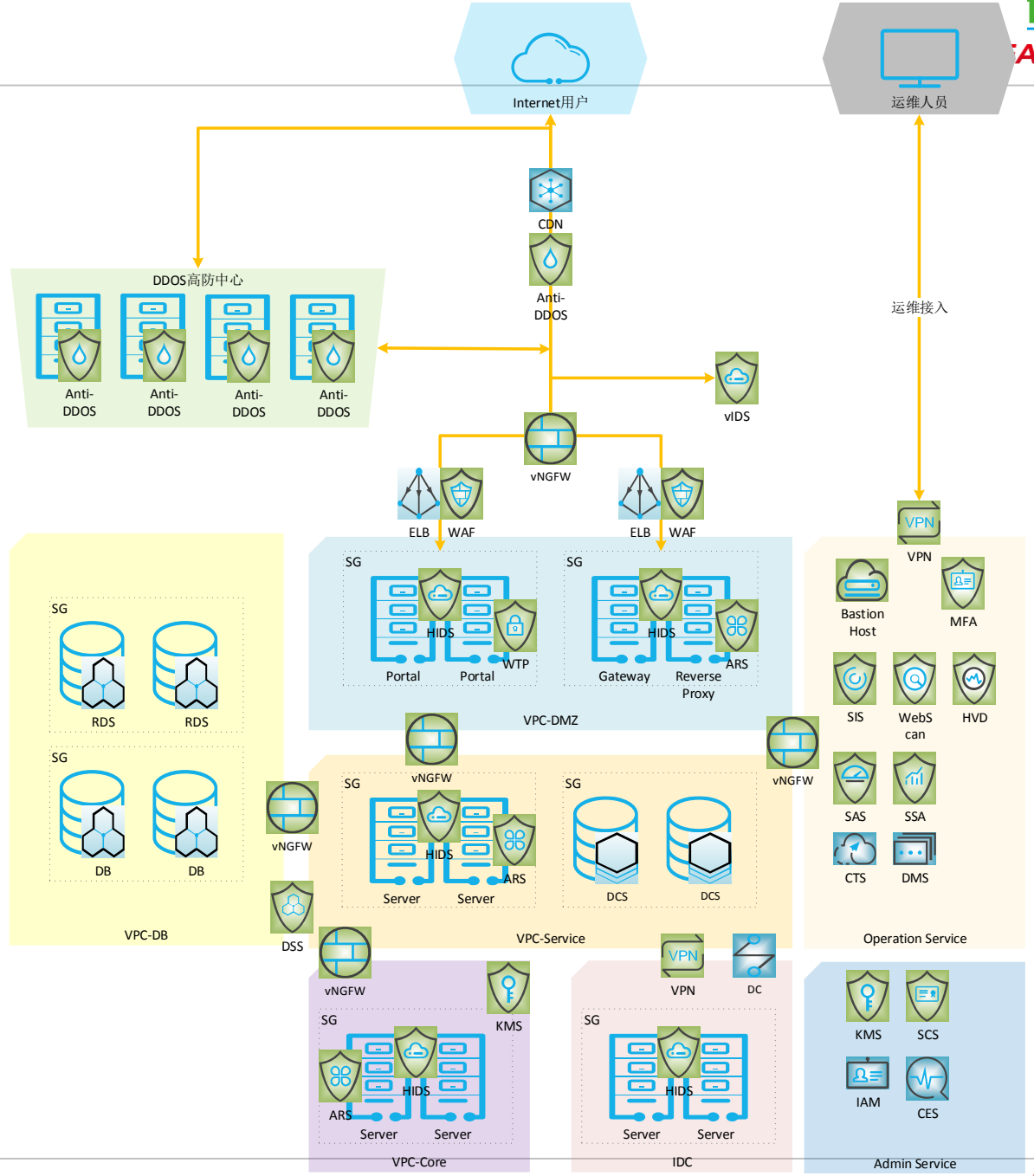
专业级数据库安全：

DSS数据库安全服务，提供含数据库防火墙、数据库审计、数据脱敏、监控等专业数据库安全特性，保障核心数据安全，1+1安全服务支持保护8个数据库，性能优异。

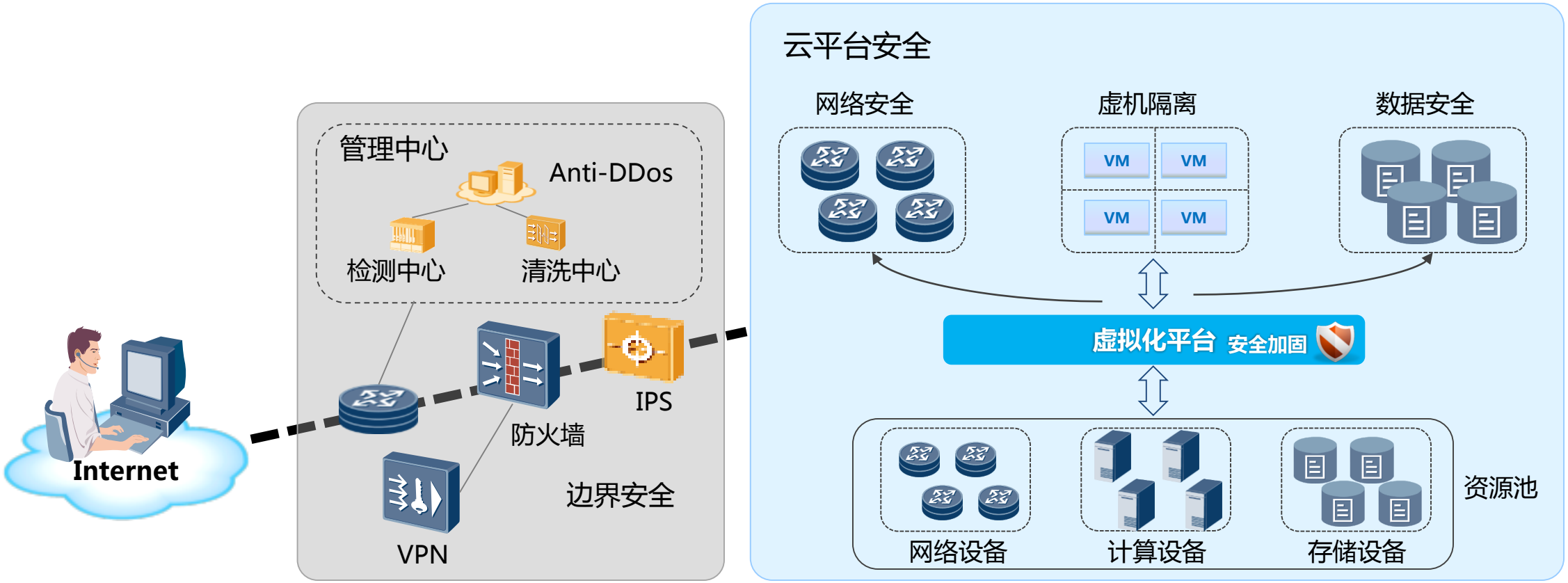
VPC： 虚拟私有云
SG： 安全组
Anti-DDOS：边界&高防DDOS
ELB： 弹性负载均衡
WAF： Web应用防火墙
vNGFW：虚拟下一代防火墙
HIDS： 主机入侵检测
vIDS：虚拟入侵检测系统
ECS： 弹性云主机
RDS： 关系型数据库
DCS： 分布式缓存服务
Bastion Host： 堡垒机
CSC： CA证书服务
SAS： 安全体检服务
SIS： 安全指数服务
ARS： 程序运行认证
KMS： 秘钥管理服务
SSA： 态势感知服务
DSS：数据库安全服务
HVD： 主机漏洞检测
WebScan： Web漏洞扫描
DC： 云专线服务

核心竞争优势：

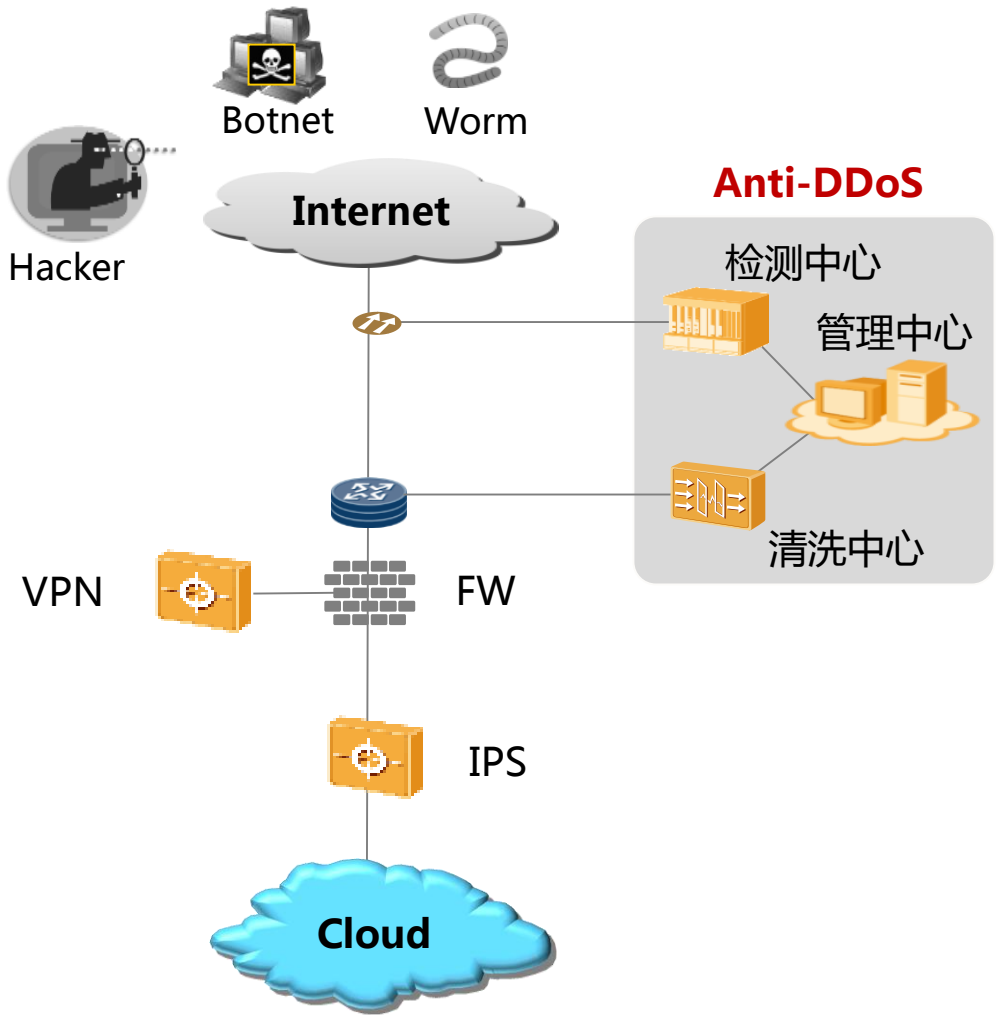
1、安全合规与可信
2、DDOS高防
3、安全隔离控制
4、纵深防御体系全方位防护
5、专业服务团队支撑
6、全面的基础安全防护



基础设施组网


管理中心
Anti-DDos
检测中心
清洗中心
Internet
防火墙
IPS
VPN
边界安全
云平台安全
网络安全
虚机隔离
数据安全
VM
VM
VM
VM
虚拟化平台
安全加固
网络设备
计算设备
存储设备
资源池

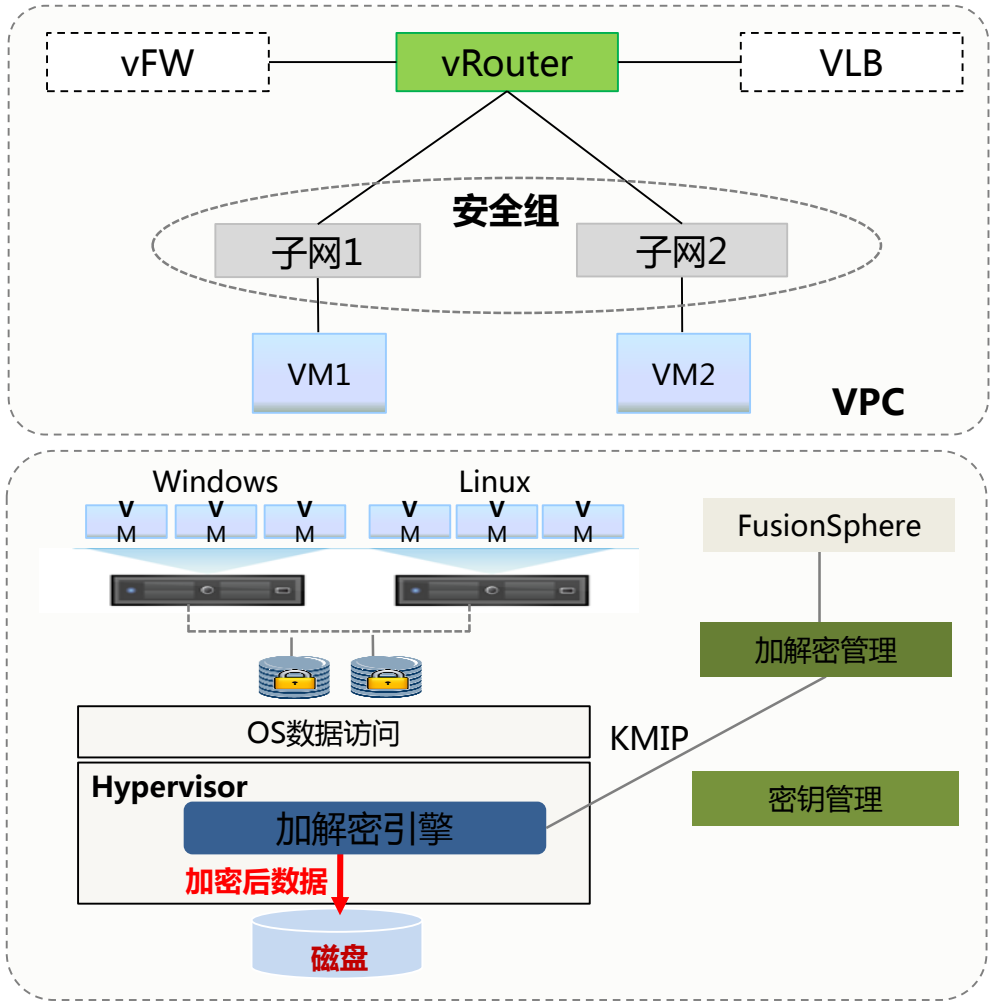
边界安全组网



防非法访问，防攻击，防拒绝服务，控制远程接入

- **专业的万兆级防火墙**：全面防护外网到云平台的非法访问，恶意攻击，病毒传播
- **精准的Anti-DDOS攻击防御方案**：精准的“V-ISA”信誉安全体系，可防御网络及应用级DDOS百余种攻击，全面解决误判，漏判；
- **深度感知的IPS解决方案**：对已知型攻击实现多重检测，全面防护；采用沙箱联动检测和信誉体系，让潜在攻击无所遁形
- **多技术远程接入方案：**支持SSL,IPSEC L2TP VPN，满足远程安全互联需求

云平台安全组网



多安全特性，按需定制防护策略

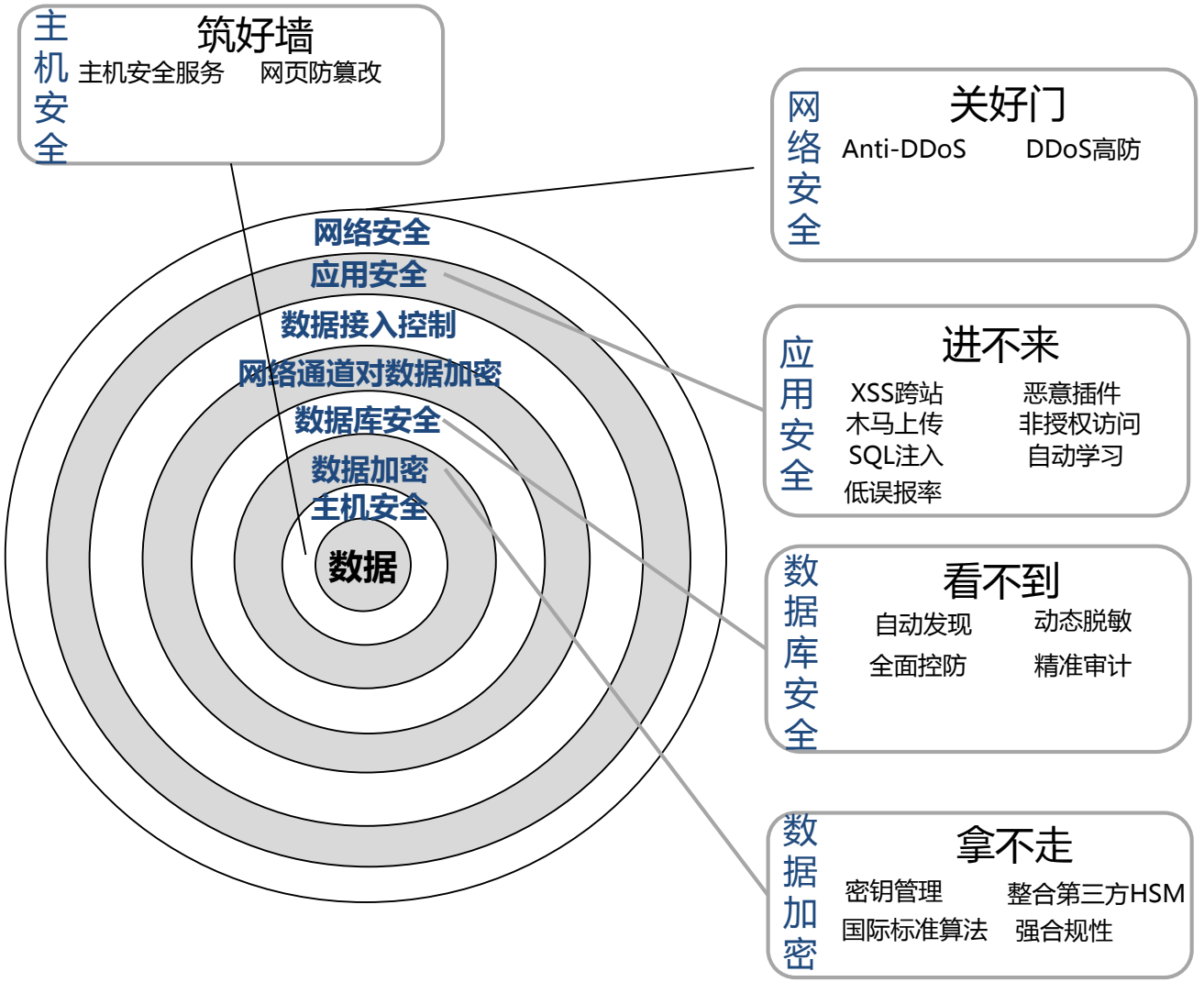
- **VPC保障VDC间网络隔离**：云平台以VPC的形式对资源进行下发，VPC内包含多种安全特性全面保护租户安全
- **双重vFW 提供网络防护**：包括硬件防火墙抽象多实例VFW, 分布式软件防火墙两种方案 ，全面解决虚拟机之间的未授权访问，恶意攻击，病毒感染
- **租户网络细化控制：**VLAN 和VxLAN实现网络二层隔离；安全组保障内部网络虚拟机访问控制

虚拟机加固，租户数据保护

- **虚拟卷加密**：提供虚拟机卷加密功能，防管理员及其他租户“恶意挂卷” 导致的 “敏感数据”丢失。
- **安全的加密算法：**支持AES,RSA,国密多种加密算法，满足加密强度高及遵循等级保护合规要求。
- **加密密钥专属硬件保存**

目录

以数据为核心构建纵深的防护体系



华为云提供的安全服务

网络安全：
- 阻挡DDoS流量攻击，提供免费的5G Mb/s四层清洗能力和20000 http/s的CC攻击
- 高防DDOSIP：单线200G，HTTPS七层防护能力
- 支持百万租户的虚拟私网隔离技术VPC

数据安全：
- 为租户应用提供等高HA硬件加密的秘钥管理服务，如OBS服务等提供数据加密选择
- 证书管理服务。
- VPN（IPSec / SSL）。

安全管理与服务：
- 一览式快速了解云环境的安全指数和态势感知，发现安全隐患
- 专业的安全体检服务，发现重大漏洞，提供专业解决方案。
- IAM统一身份认证服务。

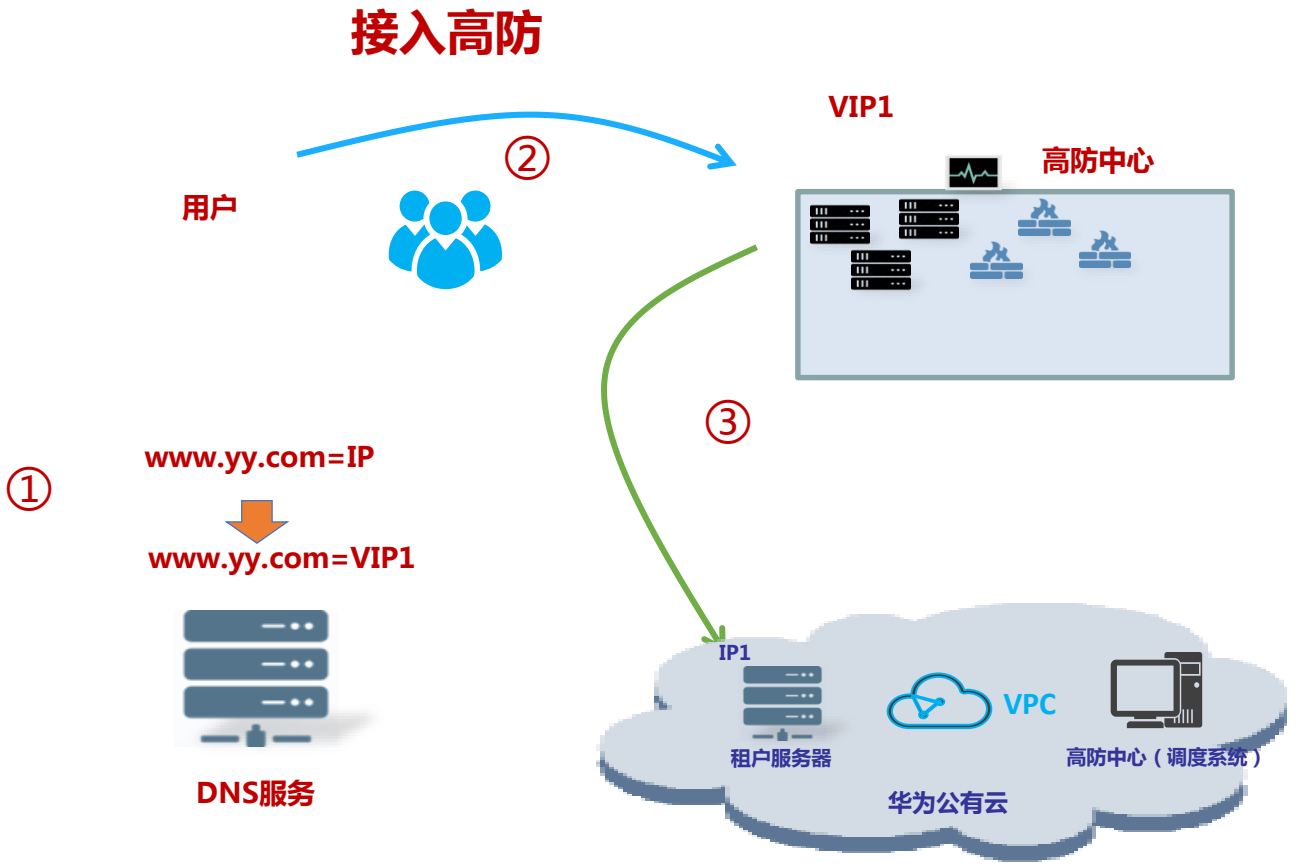
安全生态：
- 开放集成业界最优秀的安全厂商，提供全面的安全服务

应用安全：
- Web漏扫扫描， 发现网站的漏洞，帮助客户修复漏洞。
- Web应用防火墙，直接保护网站， 阻止网站被入侵。

主机安全：
- 主机防护：检查弱配置、弱口令、可疑登陆监控，提高安全性
- 程序运行认证服务：进程黑/白名单管理。
- 网页防篡改服务：对目录中的网页、电子文档、图片、数据库等文件进行保护。

专家服务：
- 提供贴身的一对一安全专家服务，提供安全防护咨询、漏洞修复、重大业务保障。

网络安全：DDoS高防IP



1. 通过更改客户域名的IP地址实现接入高防；

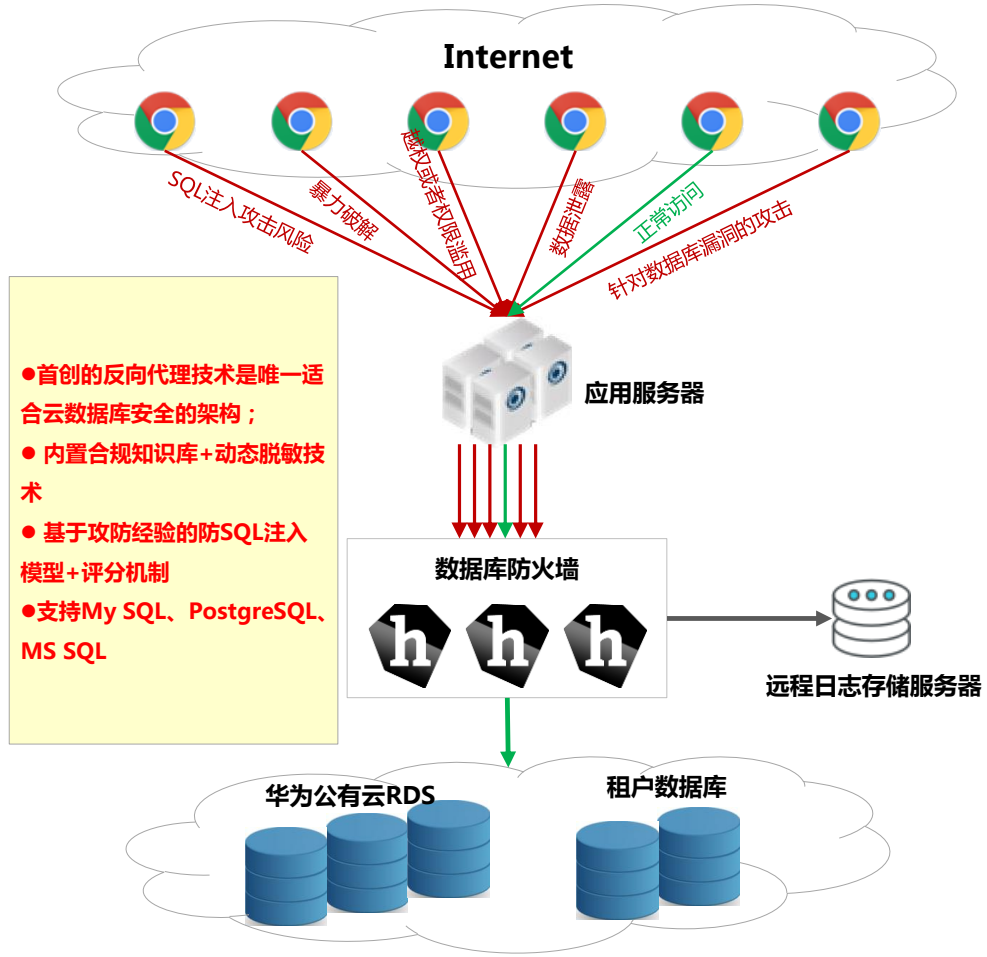
2. 流量切入高防IP；

3. 正常用户流量回源；

亮点：

- 最大300G防护能力
- 百万QPS级CC防护能力
- 电信、联通和移动多线路接入
- 基础防护（按月预付费）+弹性防护（按天后付费）

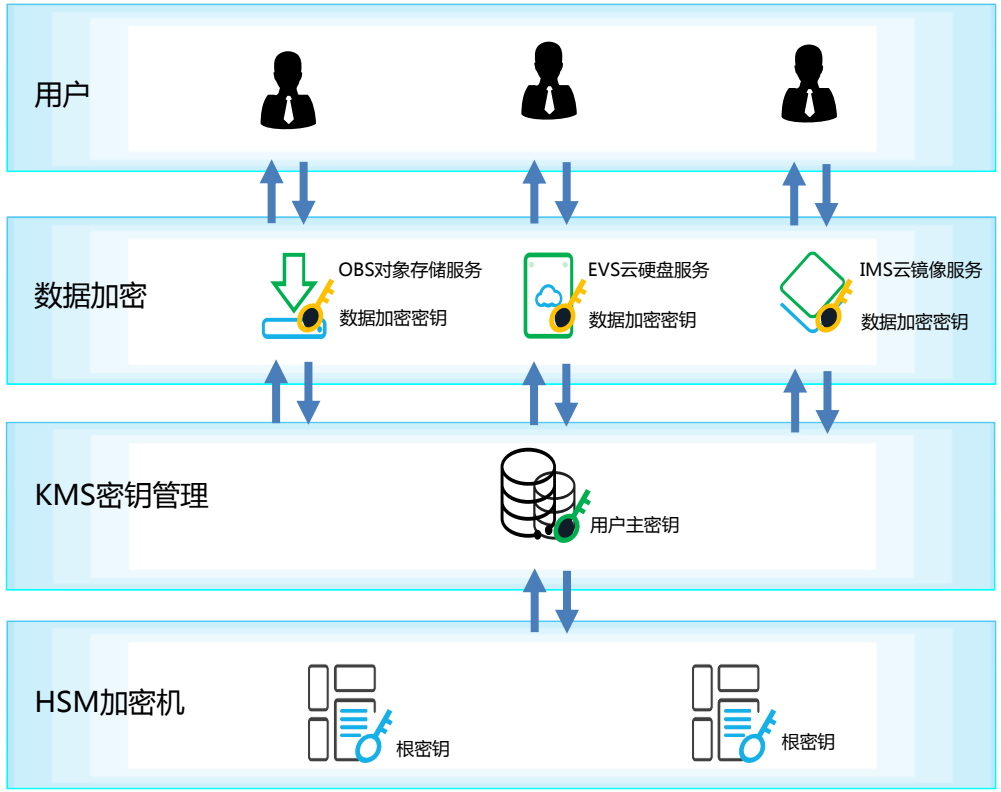
数据安全：数据库安全服务



数据库防火墙服务以反向代理模式部署在租户网络空间内，实时分析数据库的访问流量，并根据内置知识库、租户自定义规则及机器学习机制，发现和过滤违规访问和攻击行为。DBSS还提供敏感数据发现和脱敏、SQL注入检测、拖库检测、活动监控和数据库安全审计等功能。

数据安全：密钥管理服务

三层加密，保护用户数据安全



成本更低：按需付费

仅需要根据密钥个数与密钥调用次数付费，不需要为购置加密机支付额外的费用

数据加密：集成多个云服务，加密用户数据

与对象存储(OBS)、云硬盘(EVS)、云镜像(IMS)等多个基础云服务集成，实现云上数据的全面加密，集成数量国内领先

密钥管理：国内最丰富的密钥管理特性

对象存储加密

弹性块存储加密

内置审计

密钥跨租户授权

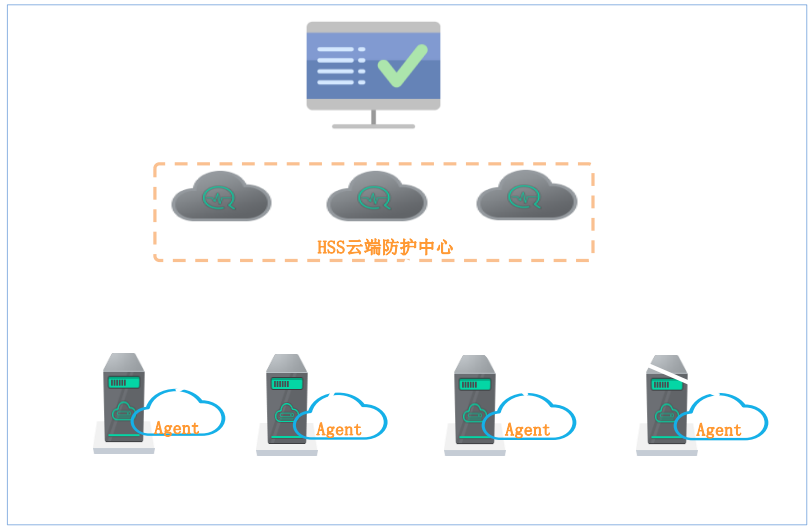
支持国内加密机

密钥保护：采用行业领先加密机作为信任根

国内唯一通过FIPS140-2认证的硬件加密模块保护密钥

主机安全：主机安全服务

主机安全服务是通过安装在主机上的插件和云端防护中心联动，来防御来自网络层、系统层和应用层的攻击，帮助用户守住最后一道防线。



全面防护　精准检测　轻量轻Agent

分类	华为云 主机安全服务关键特性	特性描述
网络防护	帐户破解防护	检测系统帐户破解攻击，并进行阻断，同时支持用户手工解封。
	异地登录检测	根据登录的IP地理位置进行检测，判别异常登录，并提示用户关注。
系统安全	弱口令检测	检测系统帐户是否存在弱口令，并提示用户进行修改
	恶意程序检测	检测系统中是否存在恶意程序，并进行报警
	开放端口检测	检测系统开放的端口，以及对应的程序信息
	系统关键文件 完整性检测	对系统关键文件（配置、命令程序）进行完整性检查，一旦被恶意篡改，立即进行报警
	系统软件 CVE漏洞	检测系统中已安装软件存在的CVE漏洞。
Web防护	网页防篡改	检测网页后门WebShell，并提示告警。

数据安全：证书管理服务

客户痛点

HTTP协议存在的问题

◆在客户端（如浏览器）与服务器端（如网站）间明文传输数据，可以被轻松截取或篡改

◆不能鉴别真实网站，欺诈、钓鱼网站导致用户信息泄露、财产损失

SSL证书作用

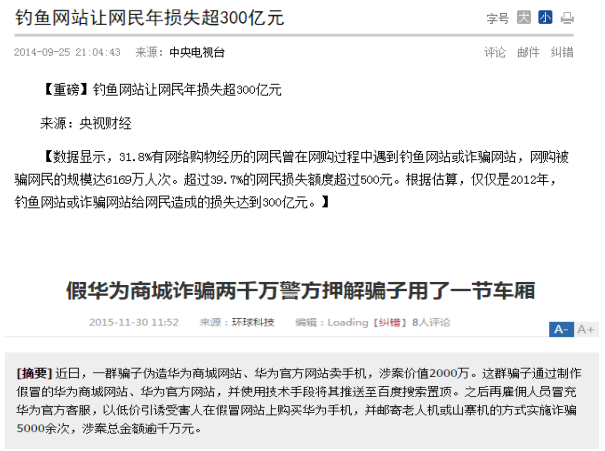
◆认证用户和服务器，确保数据发送到正确的客户机和服务器

◆在客户端（浏览器）和服务器端（网站）之间建立加密通道，保证数据在传输过程中不被窃取或篡改

应用场景

◆保障用户通信安全：防止攻击者利用HTTP协议存在的问题展开攻击，截获用户客户端与服务端通信的信息

◆防止攻击者仿冒真实网站，欺诈、钓鱼网站导致的用户信息泄露、财产损失



钓鱼网站让网民年损失超300亿元

字号 大 小

2014-09-25 21:04:43 来源：中央电视台 评论 邮件 纠错

【重磅】钓鱼网站让网民年损失超300亿元

来源：央视财经

【数据显示，31.8%有网络购物经历的网民曾在网购过程中遇到钓鱼网站或诈骗网站，网购被骗网民的规模达6169万人次。超过39.7%的网民损失额度超过500元。根据估算，仅仅是2012年，钓鱼网站或诈骗网站给网民造成的损失达到300亿元。】

假华为商城诈骗两千万警方押解骗子用了一节车厢

2015-11-30 11:52 来源：环球科技 编辑：Loading【纠错】8人评论 A- A+

【摘要】近日，一群骗子伪造华为商城网站、华为官方网站卖手机，涉案价值2000万。这群骗子通过制作假冒的华为商城网站、华为官方网站，并使用技术手段将其推送至百度搜索置顶。之后再雇佣人员冒充华为官方客服，以低价引诱受害人在假冒网站上购买华为手机，并邮寄老人机或山寨机的方式实施诈骗5000余次，涉案总金额逾千万元。

功能与价值

云端证书申请与管理

◆为降低云计算环境下证书应用的难度，提升用户体验，系统在云端提供一站式证书申请、管理服务。

集成云应用与证书服务

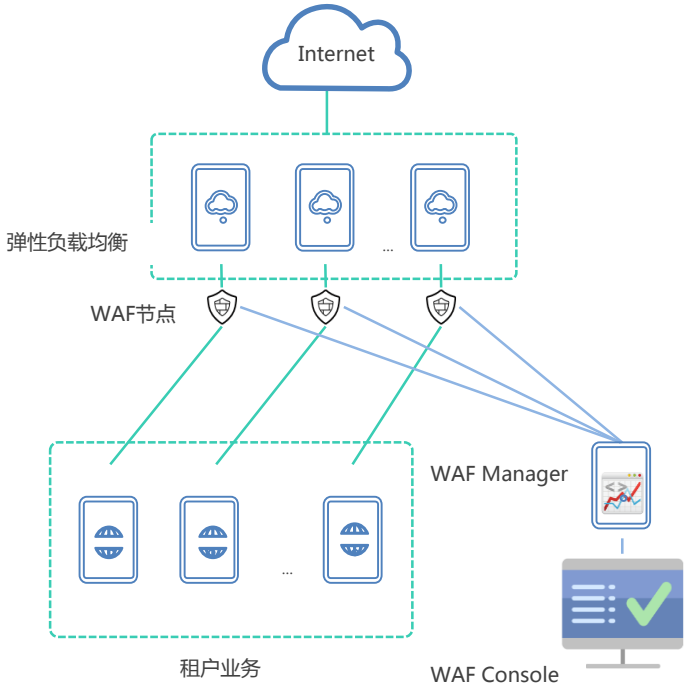
◆为提升用户在云端使用证书的便捷性，系统集成云应用与证书服务，让云应用能够直接通过证书服务实现证书操作，例如证书验证，从而提升证书服务的实用性。

应用价值

◆对用户而言：更加简便、更小成本、更为安全。

◆对平台而言：丰富产品功能、增强服务集成，提升竞争力。

应用安全：云WAF服务



CC防护场景

对象：电商、金融等行业用户
问题：当业务接口处理能力成为瓶颈被恶意访问占用大量资源时
方案：可根据IP、Cookie对用户访问请求限速处理
效果：**支持Cookie可精准识别公用一个出口IP的不同用户**

紧急漏洞修复场景

对象：电商、论坛、金融等行业用户
问题：第三方插件爆发漏洞，业务难以快速升级修复
方案：WAF通过快速下发防护规则，实现风险规避
效果：保障业务正常服务、减少业务升级成本

数据泄露场景

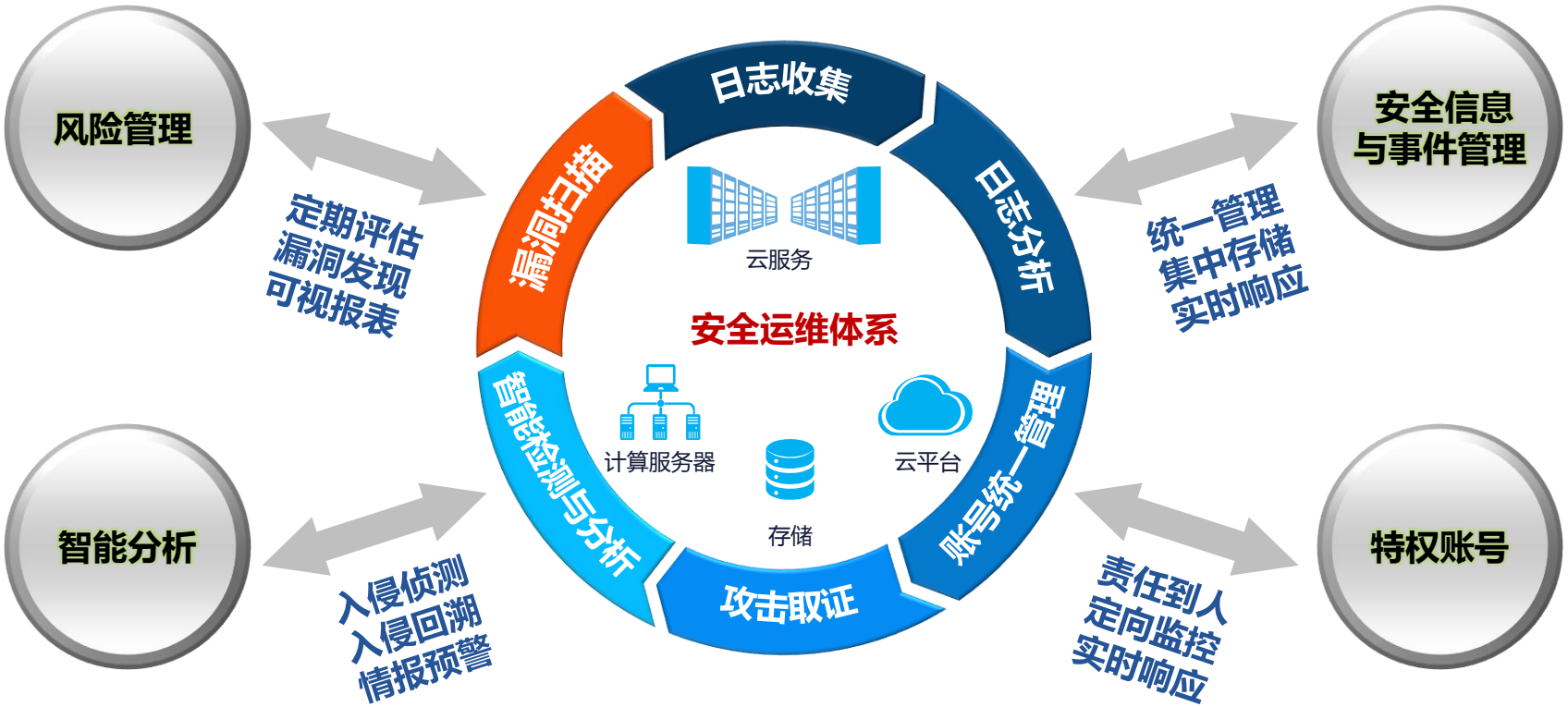
对象：电商、金融等行业用户
问题：业务的数据库、用户密码等信息可能存在泄露风险
方案：WAF可有效针对SQLi、XSS等OWSAP威胁进行防御
效果：通过语义分析防御**SQLi、XSS误报更低**
编码还原更强大，支持Unicode、hex等编码还原

精准防护场景

对象：电商、金融等企业级用户
问题：预置安全策略不能完全满足客户的定制需求
方案：可根据自身特性，自定义更复杂的规则
支持IP黑白名单、UA屏蔽等的定制规则策略
效果：业务可将自己积累的私有信誉库在waf中生效

同类服务仅支持URL encode，且缺少语义分析，误报率高

安全运维：运维体系


风险管理
定期评估
漏洞发现
可视报表
智能分析
入侵侦测
入侵回溯
情报预警
日志收集
日志分析
账号统一管理
攻击取证
智能检测与分析
漏洞扫描
云服务
安全运维体系
计算服务器
云平台
存储
安全信息
与事件管理
统一管理
集中存储
实时响应
特权账号
责任到人
定向监控
实时响应

安全运维：安全信息与事件管理

日志统一管理与关联分析

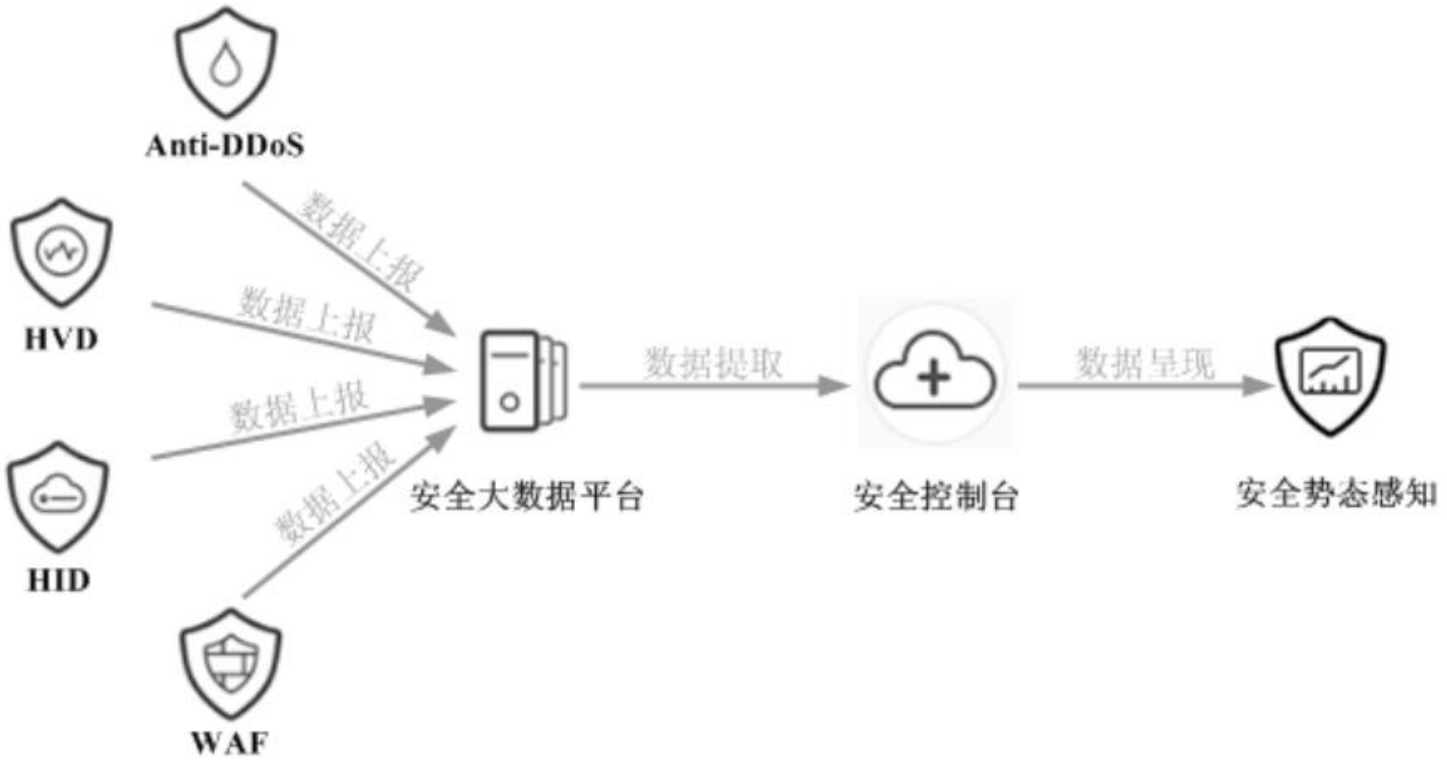
集中日志存储，提供统一的日志备份、管理，并对不同设备的日志进行关联分析，发现可能存在的攻击。

对合规提供支持

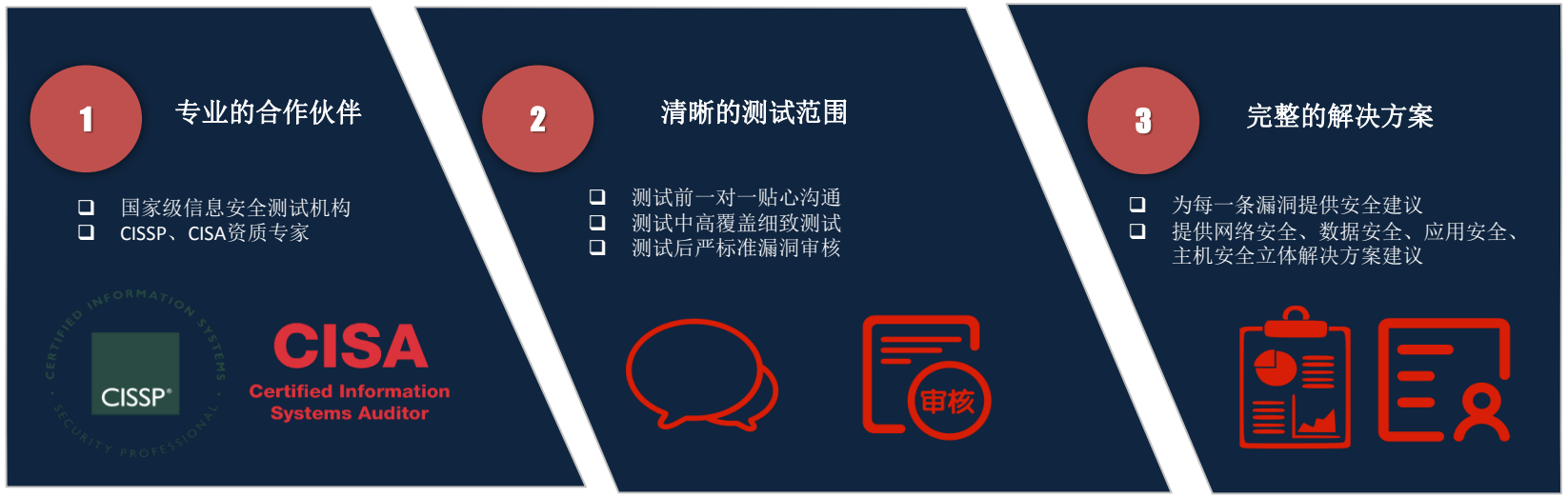
根据不同的合规要求提供报表模板，根据日志内容自动化分析合规满足程度。

态势感知服务

安全态势感知是一个数据记录、统计和分析平台，通过收集其他云安全服务的安全事 件记录，利用大数据挖掘、机器学习综合分析其各安全服务的安全事件数据、安全情 报数据，智能学习并发现潜在的入侵和高隐蔽性攻击，回溯攻击历史。帮助用户准确 理解过去发生的每一件安全事件，并为用户进行安全态势预测提供有效的依据。



安全评估：安全体检服务



下单咨询

资质核验

明确范围

购买服务

全面体检

查漏补缺

报告审核

方案建议

满足安全合规要求

认证名称	CSA STAR	ISO 27001	C-STAR	公安部信息安全等级保护	可信云	网络安全审查
适用区域	全球	国际	国际	中国	中国	中国
简介	STAR认证是由英国标准协会（BSI）与云安全联盟（CSA）联手推出，基于ISO/IEC 27001以及云控制矩阵中所规定的特定标准，是信息安全管理体系认证（ISO/IEC 27001）的增强版本，目前在该领域中认可度较高	ISO中针对企业信息安全管理的认证，全球影响力和认可度都比较高，其标准被很多其他同类型认证以及云安全认证采纳	由CSA授权独立的专业第三方审核机构赛宝专门针对中国开展的云服务安全认证	公安部对全国的信息系统的要求	数据中心联盟（工信部）要求，包括云主机、对象存储、云桌面等均已通过可信云，且已获得金牌运维	审查要求已落入网络安全法，所有政务系统的服务商强制要求满足

THANK YOU

安全生态：利用生态的力量来做好安全