华为云服务 - 云安全服务

前言

- 本章主要讲述华为云服务中的安全服务产品。

目标

- 学完本课程后，您将能够：
  - 了解云上客户的安全诉求和安全生态
  - 描述华为云安全服务产品体系
  - 掌握华为云安全服务的概念、主要功能、应用场景
  - 掌握华为云安全服务的原理与特点
  - 掌握华为云安全服务的申请和使用

目录

云上客户的安全诉求

CSA Top 威胁

- 数据泄露
- 身份、凭证和访问管理不足
- 不安全的接口和应用程序编程接口（API）
- 系统漏洞
- 账户劫持
- 恶意的内部人员
- 高级持续性威胁（APT）
- 数据丢失
- 尽职调查不足
- 滥用和恶意使用云服务
- 拒绝服务（DoS）
- 共享的技术漏洞

企业上云的关键安全诉求

业务连续不中断

- 防网络攻击
- 防黑客入侵
- 法律遵从、合规

运维全程可管控

- 配置安全策略
- 风险识别和处置
- 操作可审计、追溯

数据保密不扩散

- 防外部窃取
- 内部非授权员工不可见
- 云服务商不可见

国内法律合规要求

《网络安全法》
《网络安全等级保护制度》

第31条 国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦**遭到破坏**、**丧失功能**或**数据泄露**，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在**网络安全等级保护制度**的基础上，实行**重点保护**

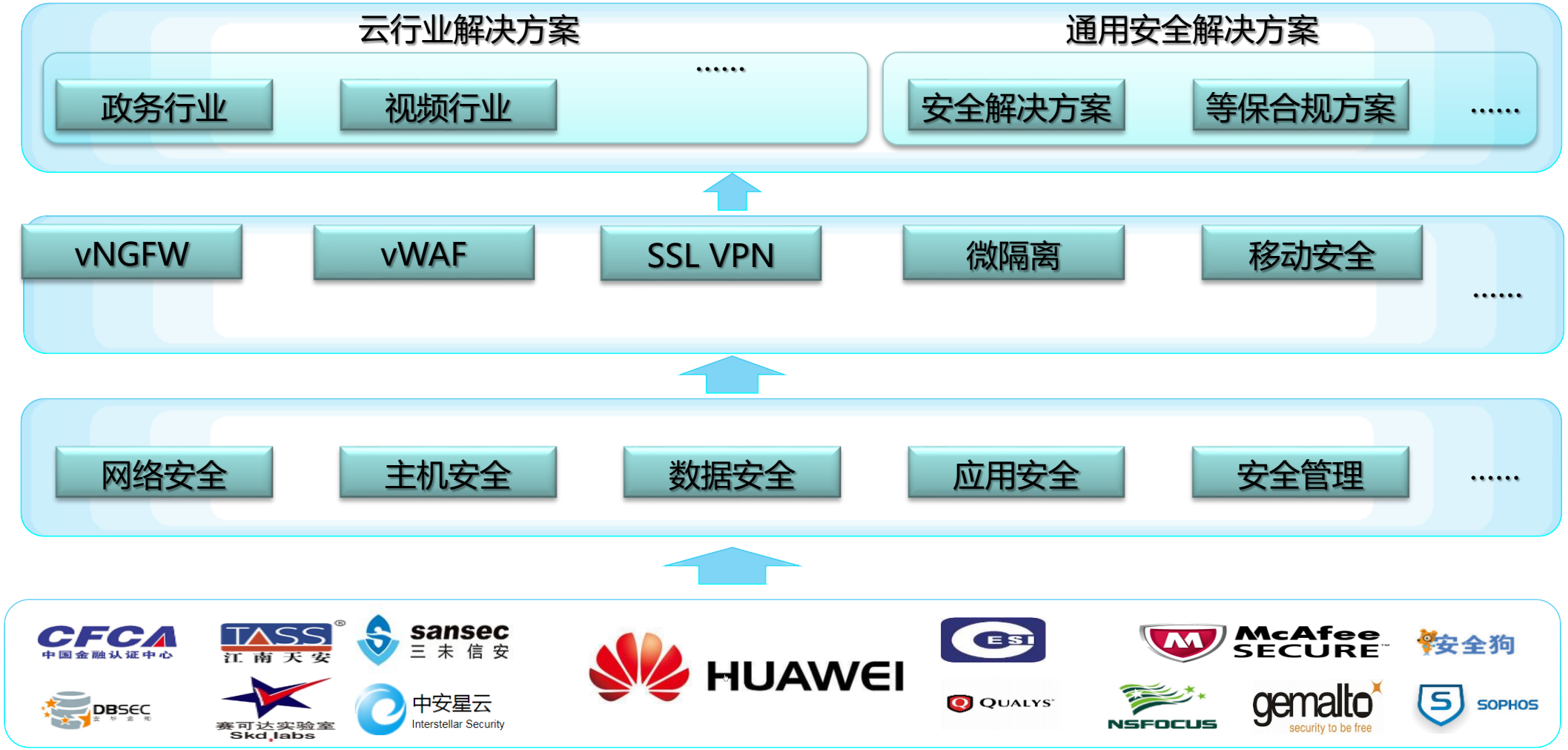
安全生态

解决方案

安全超市

安全服务

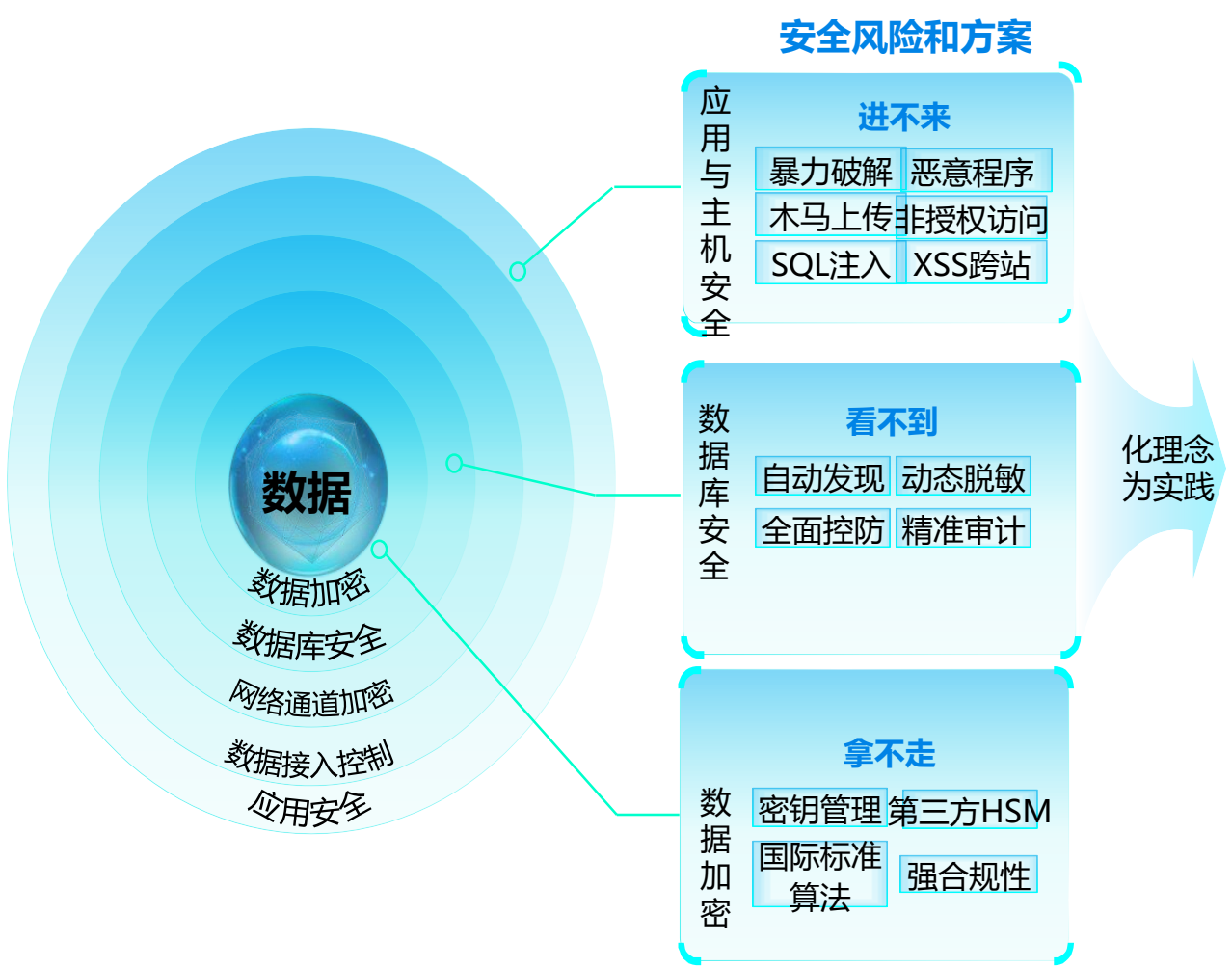
生态的基础



HUAWEI

华为云安全服务体系

以数据安全为中心，构建一系列精品安全服务



华为云安全服务产品列表 - 数据安全

安全服务	概念	主要功能	典型应用场景
数据加密服务	数据加密服务（Data Encryption Workshop）是一个综合的云上数据加密服务。它可以提供专属加密、密钥管理、密钥对管理等功能。其密钥由硬件安全模块（Hardware Security Module，HSM） 保护，并与许多华为云服务集成。用户也可以借此服务开发自己的加密应用。	• **密钥&密钥对管理**：安全、可靠、简单易用的密钥和SSH密钥对托管服务，帮助用户集中管理密钥和SSH密钥对，保护密钥和SSH密钥对的安全 • **专属加密**：专属加密服务为用户提供经国家密码管理局检测认证的专属加密实例，帮助用户保护弹性云服务器上数据的安全性和隐私性要求，满足监管合规要求。同时，用户能够对专属加密实例生成的密钥进行安全可靠的管理，也能使用多种加密算法来对数据进行可靠的加解密运算	适用于政府公共事业、互联网企业、电商等支付系统、交通、制造、医疗等 • 小数据加密 • 大量数据加密 • OBS/EVS/IMS/SFS/RDS服务端加密 • 登录Linux云服务器 • 获取Windows云服务器的登录密码 • 用户业务系统使用专属加密实例加密
数据库安全服务	数据库安全服务（Database Security Service, DBSS），是一种基于反向代理及机器学习机制，提供数据脱敏、数据库审计、敏感数据发现和防注入攻击等功能的，保障云上数据库安全的数据库安全防护服务。	• **数据库防火墙**：基于角色的访问控制，最小权限分配；SQL注入攻击防御；用户行为自学习，生成数据库防火墙策略 • **敏感数据发现与脱敏**：内置PCI-DSS/HIPAA/SOX等合规知识库，自动发现敏感数据；细粒度脱敏，行/列/表/视图级脱敏；生成遵从合规报告，方便审计 • **数据库审计**：提供行为/数据/性能异常监控；本地和远程日志的记录和存储；实时告警	适用于金融、政务、教育、医疗、保险、游戏行业等 • 帮助用户满足等保合规《网络安全法》中网络攻击和入侵防范条款，以及网络运行状态和安全事件监测防范条款 • 敏感数据泄露防护

华为云安全服务产品列表 - 主机安全

安全服务	概念	主要功能	典型应用场景
企业主机安全	企业主机安全（Host Security Service，HSS）是提升主机整体安全性的服务，为用户提供资产管理、漏洞管理、入侵检测、基线检查等功能，降低主机被入侵的风险。	账户破解防护、口令复杂度策略与经典弱口令检测、恶意程序检测、异地登录检测、关键文件变更检测、开放端口检测、软件漏洞检测 、账号和软件信息管理、Web目录管理、进程信息检测、网站后门检测、配置检测	适用于政府、事业单位、游戏、P2P、医疗等 • 帮助用户满足《中华人民共和国网络安全法》中主机入侵防范条款和主机恶性代码防范条款 • 通过事前预防、事中防御、事后检测，三位一体保护主机安全
容器安全服务	容器安全服务（Container Guard Service，CGS）能够扫描镜像中的漏洞与配置信息，帮助企业解决传统安全软件无法感知容器环境的问题；同时提供容器进程白名单、文件只读保护和容器逃逸检测功能，有效防止容器运行时安全风险事件的发生。	• **镜像漏洞管理**：扫描节点中所有正在运行的镜像，发现镜像中的漏洞并给出修复建议，帮助用户得到一个安全的镜像 • **容器安全策略管理**：通过配置安全策略，帮助企业制定容器进程白名单和文件保护列表，从而提高容器运行时系统和应用的安全性 • **容器逃逸检测**：扫描所有正在运行的容器，发现容器中的异常（包括逃逸漏洞攻击、逃逸文件访问等）并给出解决方案	适用于大企业、游戏、生物基因、科学计算、金融、媒资、能源、旅游等 • 镜像漏洞扫描：保证容器使用的是安全的镜像 • 监控容器运行时的安全状态：保护容器安全

华为云安全服务产品列表 - 应用安全

安全服务	概念	主要功能	典型应用场景
Web应用防火墙	Web应用防火墙（Web Application Firewall， WAF），通过对HTTP(S)请求进行检测，识别并阻断SQL注入、跨站脚本攻击、网页木马上传、命令/代码注入、文件包含、敏感文件访问、第三方应用漏洞攻击、CC攻击、恶意爬虫扫描、跨站请求伪造等攻击，保护Web服务安全稳定。	• Web应用攻击防护：覆盖OWASP（Open Web Application Security Project）TOP 10中常见安全威胁，通过预置丰富的信誉库，对恶意扫描器、IP、网马等威胁进行检测和拦截 • CC攻击防护、精准访问防护、扫描器爬虫防护、地理位置访问控制、网页防篡改、网站反爬虫、防敏感信息泄露	• 常规防护：防数据泄露、防网页篡改 • 电商抢购秒杀防护 • 0 Day漏洞爆发防护
漏洞扫描服务	漏洞扫描服务（Vulnerability Scan Service，简称VSS）是针对服务器或网站进行漏洞扫描的一种安全检测服务，目前提供通用漏洞检测、漏洞生命周期管理、自定义扫描多项服务。	• **多元化检测**：包括但不限于Web应用、主机、中间件、弱密码检测 • **紧急漏洞检测**：监控业界最新漏洞，第一时间扫描资产是否存在最新漏洞 • **周期性风险检测**：定时定期检测资产的安全风险 • **弱密码检测**：支持标准Web业务弱密码检测、操作系统、数据库等弱口令检测	广泛适用于有漏洞扫描需求的行业，如：政府单位、金融、教育、医疗、保险、交通、电商、游戏等 • 一键检测最新CVE漏洞 • 检测企业弱密码

华为云安全服务产品列表 - 网络安全

安全服务	概念	主要功能	典型应用场景
Anti-DDoS流量清洗	Anti-DDoS流量清洗服务（以下简称Anti-DDoS）为华为云内资源（弹性云服务器、弹性负载均衡和裸金属服务器），提供网络层和应用层的DDoS （Distributed Denial of Service）攻击防护和攻击实时告警通知。同时，Anti-DDoS可以提升用户带宽利用率，确保用户业务稳定运行。	• DDoS攻击防护 • 为单个弹性IP地址提供监控记录 • 为保护的弹性IP地址提供拦截报告	• 网站类应用场景：网站类业务属于DDoS攻击的重灾区，攻击者可通过大流量攻击或应用层CC攻击，导致网站访问缓慢甚至瘫痪；Anti-DDoS可抵御4-7层攻击，提升网站访问体验。 • 游戏类应用场景：游戏行业恶意攻击频发，DDoS清洗服务防御各种基于在线游戏的DDoS攻击，如空连接、慢连接、CC攻击、踢人外挂及针对游戏网关和战斗服务器的攻击。
DDoS高防	DDoS高防（Advanced Anti-DDoS，AAD）是基于Anti-DDoS清洗设备和大数据运营平台构建的DDoS防护服务，通过流量转发方式对用户源站进行隐藏保护。	• 防护大流量DDoS攻击 • 提供配置转发规则功能 • 提供域名接入方式 • 设置告警通知 • 提供查看DDoS高防线路（目前支持电信、联通、移动、BGP线路）的流量防护、网站防护以及安全统计信息 • 提供查看DDoS高防线路的防护报表	适用于游戏、金融、电商等用户防御大流量的DDoS攻击。

华为云安全服务产品列表 - 安全管理 (1)

安全服务	概念	主要功能	典型应用场景
安全专家服务	安全专家服务（Security Expert Service，SES）是华为与第三方权威机构一起为客户提供的“专家式”人工服务，帮助客户预防、监测、发现主机、站点及系统的安全风险，给出解决方案及权威报告，并及时修复被攻击系统，降低损失。此外，还可以提供等保安全等一站式服务。	提供以下三类安全专家服务。 • **标准版**：提供网站安全体检、主机安全体检、安全加固、安全监测和应急响应5种服务类型 • **企业版**：提供安全咨询、安全体检、安全加固、安全巡检、应急响应和安全产品托管一站式的安全专业服务 • **等保安全**：为客户量身定制等保合规整改建议，指导客户进行安全服务的选型和部署，对网络、主机、数据库、安全管理制度等进行整改，优选具有资质的权威等保测评机构，提供专业的测评服务	适用于政府、财税、教育、电信、能源、交通、游戏、金融、大企业等 • 帮助用户满足《中华人民共和国网络安全法》中网络安全等保条款 • 通过事前预防（安全体检、安全监测）、事中（应急响应）、事后（安全加固）的专家式服务，三位一体保护企业的安全

华为云安全服务产品列表 - 安全管理 (2)

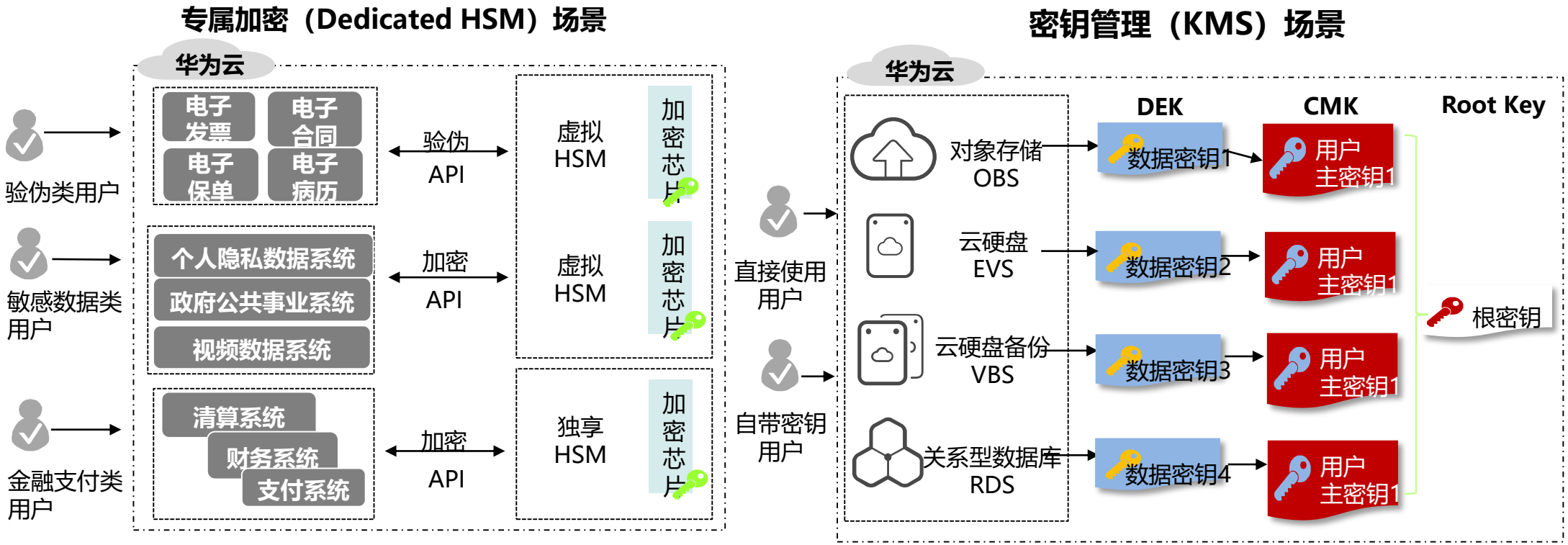
安全服务	概念	主要功能	典型应用场景
态势感知	态势感知（Situation Awareness, SA）为用户提供统一的威胁检测和风险处置平台，帮助用户检测云上资产遭受到的各种典型安全风险，还原攻击历史，感知攻击现状，预测攻击态势，并为用户提供强大的事前、事中、事后安全管理能力。	• **数据采集**：在华为云出入口部署流探针和入侵检测系统采集网络流量，同时收集DDoS、Web防火墙、主机安全等安全设备的日志到安全威胁分析平台 • **威胁发现**：建立不同的威胁模型，通过大数据进行学习分析，可以识别约30种主要安全威胁 • **集中呈现**：集中呈现租户资产的安全状态 • **威胁分析**：提供基于被攻击资产视角的威胁分析和基于攻击源视角的威胁分析，及时调整安全策略 • **安全编排**：针对已检测出来的安全威胁，一键式生成和下发安全策略，与安全防御产品形成安全联动	适用于金融、政务、教育、医疗、保险、游戏行业等 • 总览安全态势 • 定期审视资产安全状况 • 详细查看威胁事件细节 • 多维度了解主机安全态势 • 使用大屏投屏，实时展示安全情报 • 安全编排 • 威胁事件发生后及时获得通知
SSL证书管理	SSL证书管理（SSL Certificate Manager，SCM）是一个SSL证书管理平台，可供用户购买SSL证书，及上传本地的外部SSL证书到平台，实现内外部SSL证书集中管理。	提供6种类型的SSL证书。	适用于网站、APP等，提升网站安全性、网站品牌好感度、SEO搜索排名 • 企业型OV：中小型企业 • 增强型EV：有严格安全要求的企业 • 域名型DV：个人网站企业测试

华为云安全服务的申请与使用

- 华为云提供统一的管理控制台
- 用户可根据自身的安全需求开通适合的安全服务
- 安全服务可单独使用，也可组合使用
- 云服务操作日志可在“管理与部署 > 云审计服务”中查询
- 安全告警可根据用户需求通过短信、邮件等方式提供

目录

云安全服务 - DEW

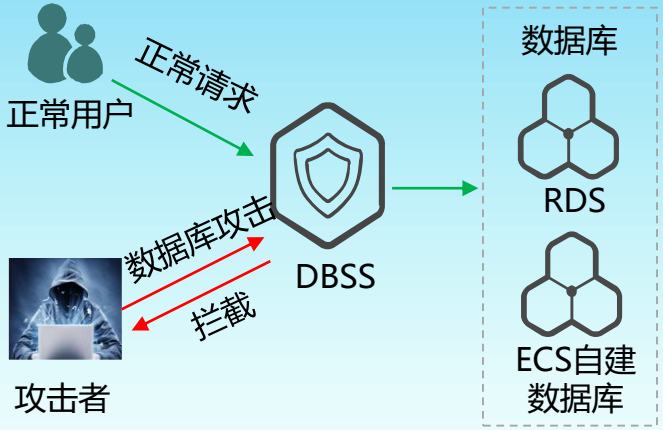


- 高安全性：只有租户可以访问和操作，数据可控
- 独享芯片加密：保障业务性能和高并发处理，无延迟
- 合规性满足：支持国密算法或FIPS140-2 Level 3认证

- 集成度高：无二次开发，节省人力，方便快捷
- 高安全性：支持用户自带密钥，云服务商不掌握
- 海量密钥管理：支持密钥定期自动轮转，满足大企业内控

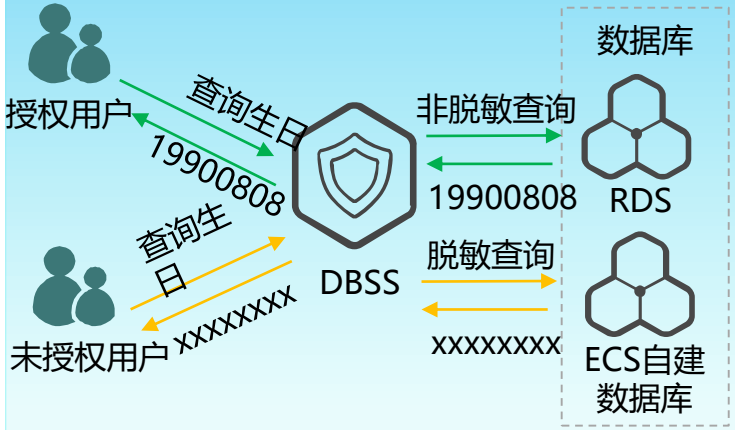
云安全服务 - DBSS

数据库防火墙场景



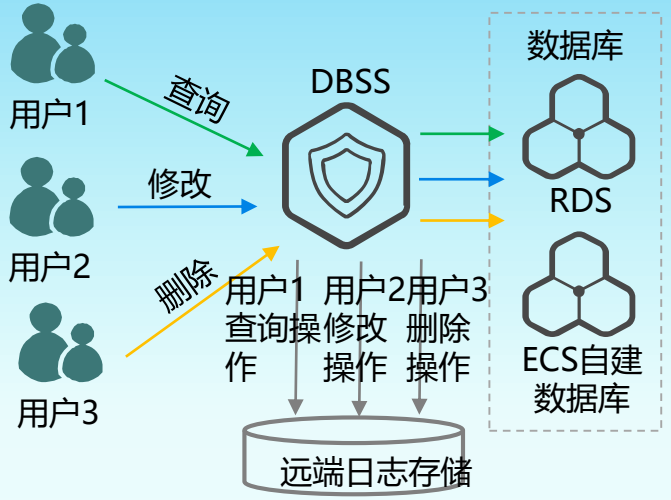
- **数据库入侵防御**：实时阻断SQL注入攻击等；
- **细粒度访问控制**：基于角色、最小化权限；
- **学习模式**：通过自我学习，生成安全模式，可应用到防火墙策略。

敏感数据发现和脱敏场景



- **敏感数据自动发现**：根据合规要求自动发现敏感数据，一键生成脱敏规则；
- **动态脱敏**：不修改原始数据，可对列脱敏；
- **多种脱敏规则**：邮箱脱敏、字符串脱敏等。

数据库审计场景



- **活动及异常监控**：列表级管理活动和访问活动监控，行为/登录/访问异常监控；
- **实时告警**：SQL注入等实时告警；
- **审计报告**：可生成合规审计报告

当前支持的数据库类型：SQL Server 2008 – 2014、MySQL 5.5 - 5.7、PostgreSQL 9.4 - 9.5

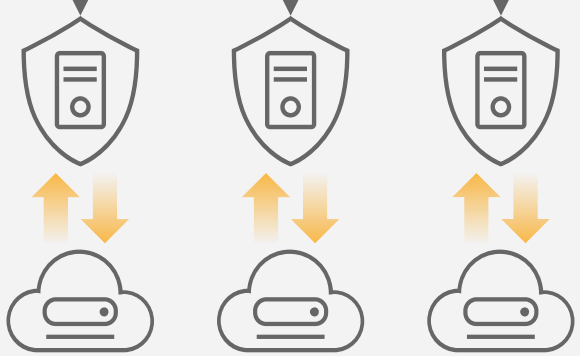
云安全服务 - HSS

主机安全管理中心 Console

统一安全管理

主机安全 Agent

云上/云下主机



*支持华为云、混合云、其他公有云、私有云、数据中心部署

- 资产管理
- 漏洞管理
- 基线检查
- 入侵检测

安全风险管理

- 资产、配置、漏洞精准检测
- 安全风险可视化，态势可感知
- 安全资产变动实时通知

企业安全合规

- 业界标杆的10+配置基线检查
- 满足等保合规测评要求
- 满足PCI-DSS文件完整性要求

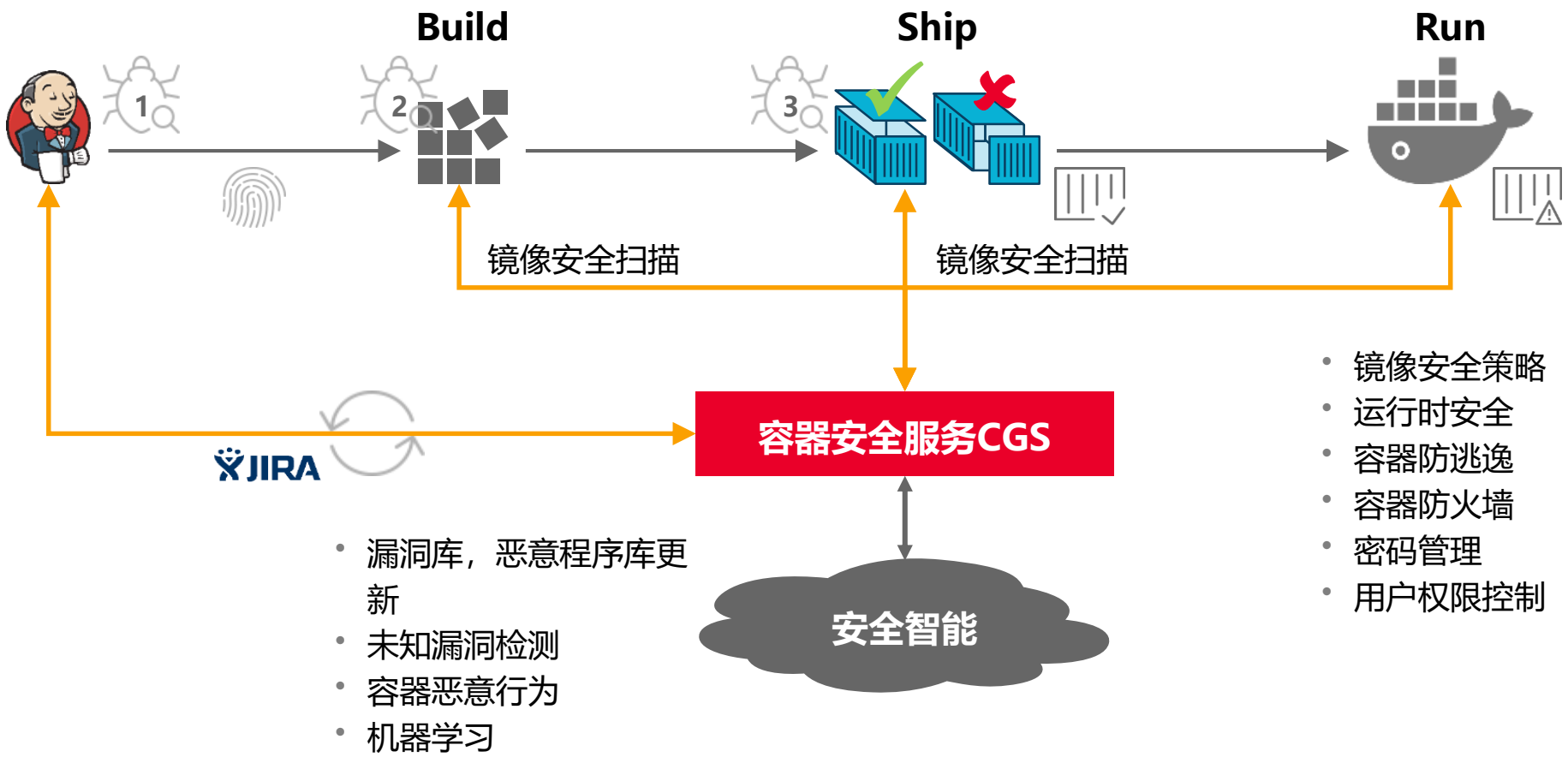
智能入侵检测

- 双因子认证预防暴力破解
- 基于AI检测引擎，有效查杀病毒、木马、挖矿、后门等
- 网页防篡改（实时阻断+恢复）

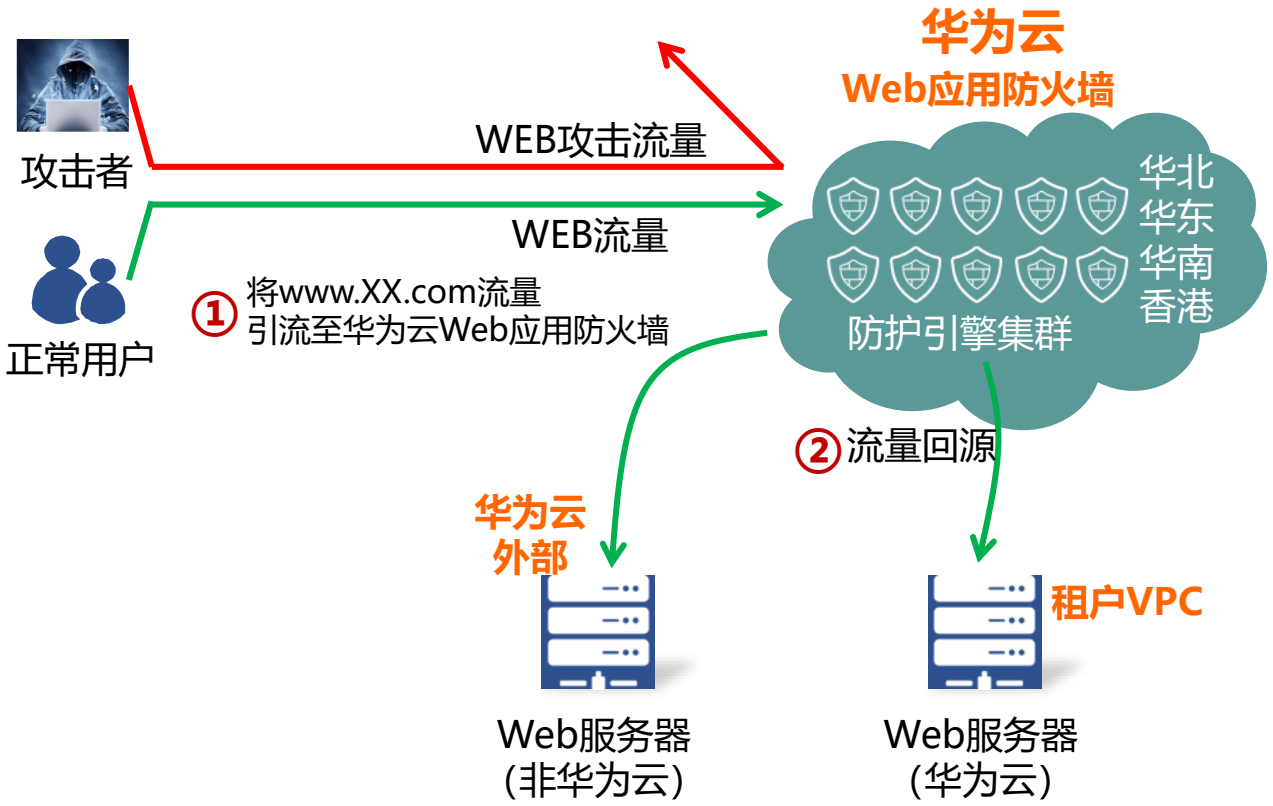
大企业50000+同时稳定运行实践，减少90%被攻击次数，100%保护主机安全

云安全服务 - CGS

容器安全服务：保证容器环境全周期安全



云安全服务 - WAF



WAF的主要好处就是可以防范企业开发的Web应用代码中“自己造成的”安全漏洞，并且防范主流Web应用软件中的安全漏洞。

技术创新

- **三引擎架构：** 独创语义+正则+AI三引擎架构，威胁检出率**提升30%以上**
- **动态防爬虫：** **领先**基于加密技术的防爬虫算法，有效防止爬虫导致的数据泄露
- **防CC：** **领先**IP+Cookie+Referer三重验证阻断CC攻击，有效提升业务可用性

专业可靠

- **国内异地容灾：** 确保业务不中断
- **实时监控：** 专业运营团队7*24小时监控
- **隐私保护：** 防止租户隐私泄露

简单易用

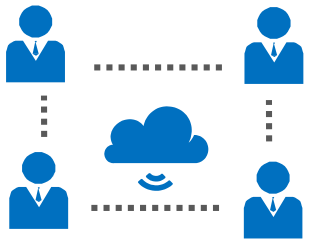
- **零维护成本：** 无组件安装，零运维
- **极简UI：** 界面简洁易懂
- **专家咨询：** 安全专家在线答疑解惑

云安全服务 - VSS

- ✓ 在线扫描，即开即用
- ✓ 操作简便，一键扫描

- ✓ 智能扫描，业务分析
- ✓ 实时监控，动态调频

- ✓ 可自定义扫描设置
- ✓ 满足不同场景扫描需求

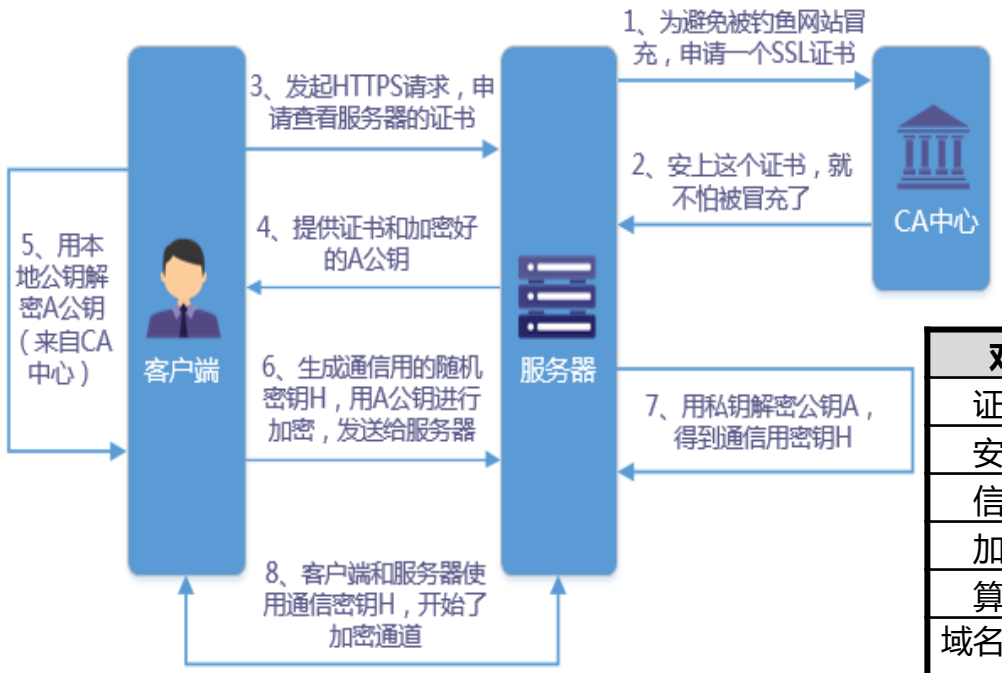


- ✓ 协同云上安全服务
- ✓ 共筑立体安全体系

关键特性	说明
漏洞检测	支持常见OWASP漏洞检测，支持三十多种漏洞类型检查，包括但不限于：Web注入漏洞、文件包含漏洞、配置错误、信息泄露、后门植入等
业务威胁	针对网站业务风险等进行风险监控和扫描，包括但不限于：网页敏感内容、垃圾广告、网页挂马、恶意外链等
等保配置	对标等保合规标准对基线配置合规等问题进行扫描，形成专业扫描报告，方便用户比对优化
漏洞报告	针对扫描结果形成专业的风险扫描报告，提供在线查看，同时也支持下载，方便内部传递信息细节
紧急CVE	安全专家7*24小时实时监控安全动态，第一时间更新紧急漏洞扫描规则，在最短时间内实现紧急漏洞扫描

云安全服务 - SCM

SSL证书管理：实现网站和应用的安全传输



提升网站安全性

使用了 SSL证书进行网站数据传输加密，可保护网站和用户间的通信数据，降低数据和流量被劫持的可能。

提升SEO搜索排名

百度、谷歌等搜索引擎，SEO搜索排名更倾向于使用了SSL证书的安全网站。

提升网站品牌好感度

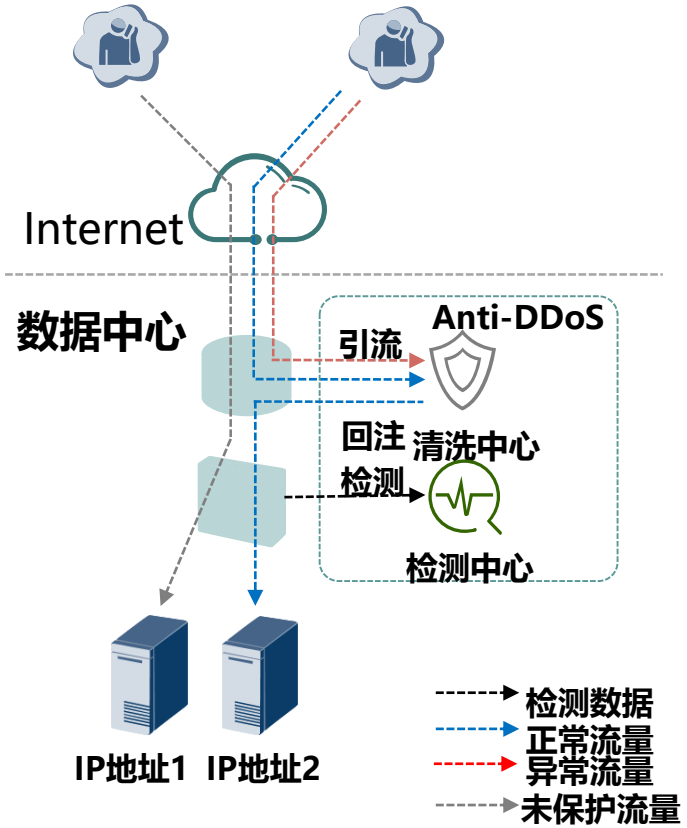
绿锁标识提示网站有着良好的安全性。若网站部署高版本SSL证书，还会显示网站品牌名，提升用户信任感和品牌好感度。

对比项	测试证书	商用证书	商用证书	商用证书	商用证书
证书类型	域名型DV	企业型OV	企业型OV Pro	增强型EV	企业型EV Pro
安全等级	★★	★★★	★★★★	★★★	★★★★★
信任等级	★	★★★	★★★	★★★★	★★★★★
加密强度	支持256位	支持256位	支持256位	支持256位	支持256位
算法支持	RSA	RSA	ECC/RSA	RSA	ECC/RSA
域名所有审核权	RDS验证	RDS或邮箱验证	RDS或邮箱验证	RDS或邮箱验证	RDS或邮箱验证
企业审核	—	组织机构验证	组织机构验证	最强组织验证	最强组织验证
小绿锁,https	√	√	√	√	√
显示企业名称	—	—	—	√	√
保障赔付	—	最高$1500000	最高$1500000	最高$1500000	最高$1500000
应用场景范围	★	★★★	★★★	★★★★	★★★★★
获证周期	自动签发	3-5工作日	3-5工作日	7-10工作日	7-10工作日

云安全服务 - Anti-DDoS

Anti-DDoS为用户提供高可靠、高安全、按需使用、弹性扩展的DDoS攻击防范服务，保障华为云内资源（弹性云服务器、弹性负载均衡和裸金属服务器）的可持续运行。

部署架构与工作原理



Anti-DDoS设备部署在网络出入口

检测中心根据用户配置的安全策略，检测网络访问流量

当发生攻击时，将数据引流到清洗设备进行实时防御，清洗异常流量，转发正常流量

可防范的攻击类型

1. **畸形包、探测包过滤**
2. **基于网络传输的攻击防护**：有效抵御SYN/SYN-ACK/FIN/RST Flood攻击，UDP Flood攻击，ICMP Flood，TCP连接耗尽攻击等
3. **基于应用层的威胁防护**：有效抵御HTTP Get/Post Flood攻击，CC 攻击，HTTP Slow Header/Post，HTTPS Flood攻击等

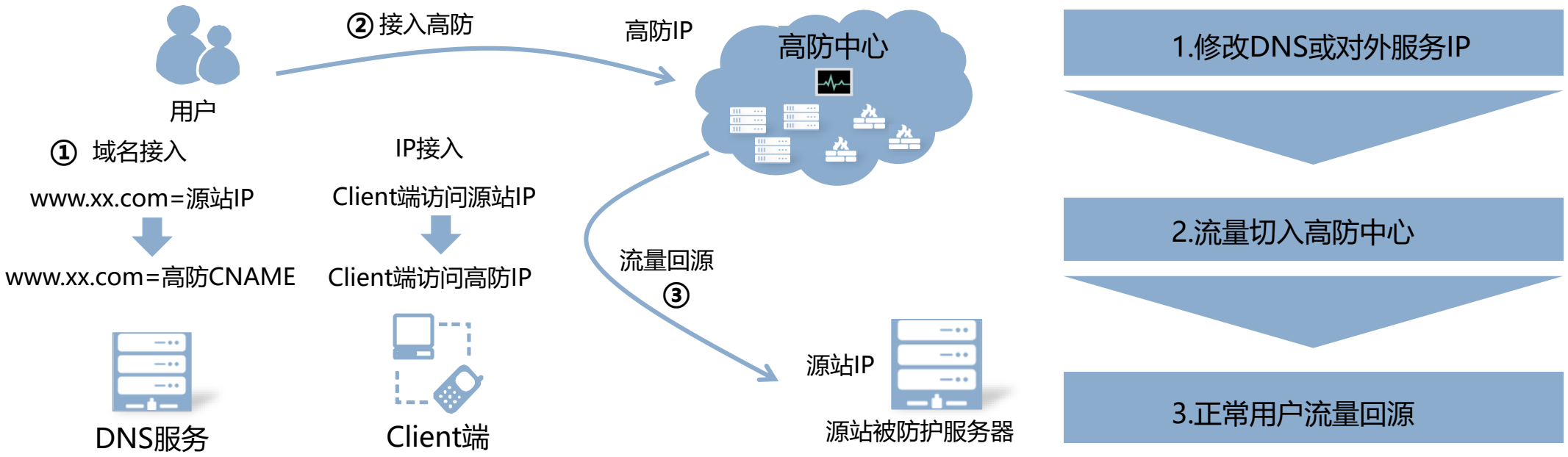
可防范的攻击规模

1. 免费5Gbps DDoS攻击防护
2. 秒级攻击防护响应

注：华为云可根据业务要求不断提升服务的功能性能

云安全服务 - DDoS高防

DDoS高防产品是针对解决互联网服务器（包括非华为云主机）在遭受大流量的DDoS攻击后导致服务不可用的情况，推出的付费增值服务。您可以通过配置DDoS高防IP，将攻击流量引流到高防IP，确保源站的稳定可靠。



云安全服务 - SES

专业资质的品质保障

- 国家信息安全测评中心合作
- CISSP、CISA资质专家服务

CISA
Certified Information Systems Auditor

企业版

- 安全咨询
- 安全加固
- 应急响应
- 安全体检
- 安全巡检
- 安全产品托管

网站安全体检

检测网站威胁，覆盖SQL注入、XSS跨站、文件上传/下载/包含、敏感信息泄露、弱口令等

主机安全体检

通过日志分析、漏洞扫描等识别主机威胁，通过基线检查发现主机OS、中间件的错误配置、不合规项和弱口令等风险

安全监测

提供六个维度的网站监测：网页木马、恶意篡改、坏链、对外开放服务、可用性、脆弱性等，支持HTTP/HTTPS协议监测

应急响应

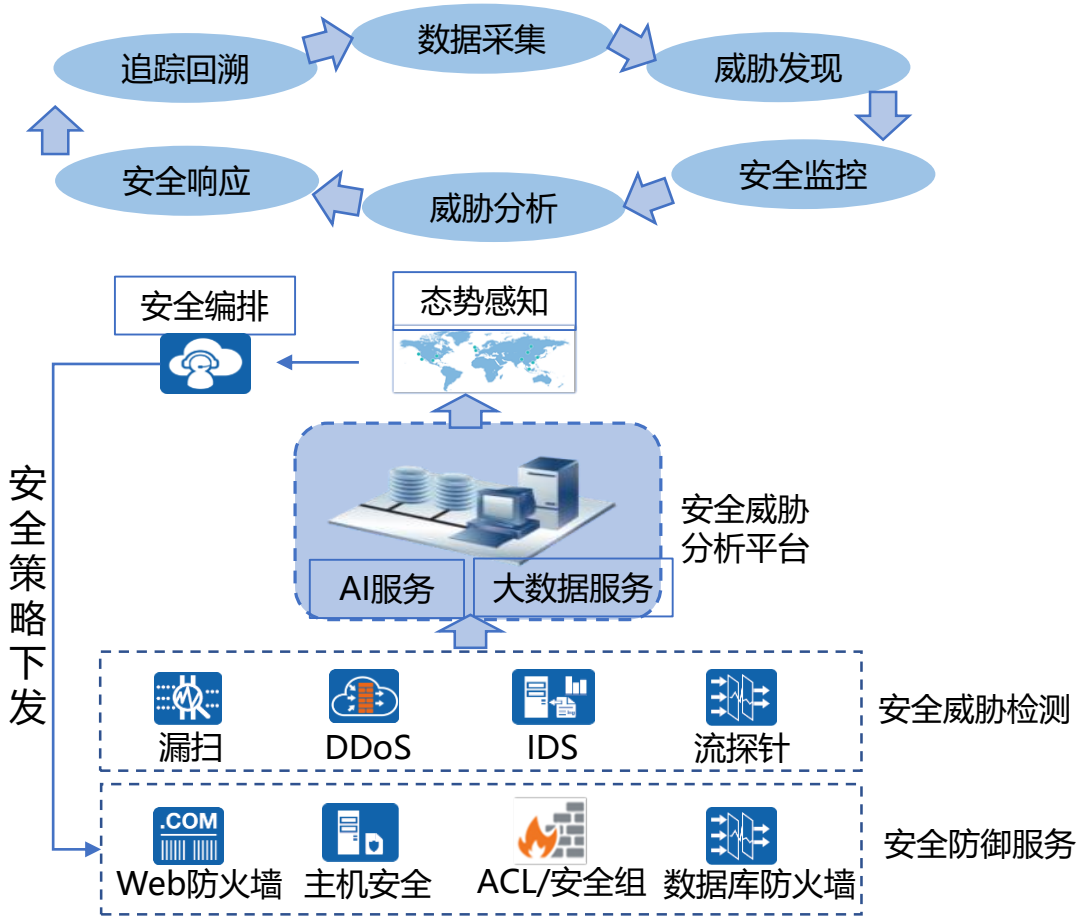
安全专家远程提供事件处置服务，包括主机系统内的恶意程序及Web系统内的可疑文件，帮助企业快速恢复业务

安全加固

对主机服务器、中间件进行漏洞扫描，分析OS和组件版本，提供整改建议，授权下完成漏洞的修复和组件的加固

云安全服务 - SA

集风险发现、风险应对、风险管理于一体



态势感知

(Situation Awareness)

通过大数据分析为用户提供统一的威胁检测和风险处置平台。

- **数据采集**：在华为云出入口部署流探针和入侵检测系统采集网络流量，同时收集DDoS、Web防火墙、主机安全等安全设备的日志到安全威胁分析平台
- **威胁发现**：建立不同的威胁模型，通过大数据进行学习分析，可以识别约30种主要安全威胁
- **集中呈现**：态势概览能够集中呈现租户资产的安全状态，实时监控整体安全状态
- **威胁分析**：提供基于被攻击资产视角的威胁分析和基于攻击源视角的威胁分析，及时调整安全策略
- **安全编排**：针对已检测出来的安全威胁，一键式生成和下发安全策略，与安全防御产品形成安全联动

思考题

1. 为保障网站安全，可以选择使用哪些安全服务？(多选)

   A. Web应用防火墙

   B. 漏洞扫描服务

   C. SSL证书管理

   D. Anti-DDoS流量清洗

本章总结

- 描述了华为云服务中安全服务产品
- 讲解了云安全服务的概念、功能、场景、原理、特点
- 讲解了云安全服务的申请和使用

学习推荐

- 华为Learning网站
  - http://support.huawei.com/learning/Index!toTrainIndex
- 华为Support案例库
  - http://support.huawei.com/enterprise/servicecenter?lang=zh
- 华为云官方网站
  - https://www.huaweicloud.com
- 华为云帮助中心
  - https://support.huaweicloud.com


谢 谢
www.huawei.com