HUAWEI

HUAWEI IT大咖说 知识共享平台

华为云技术私享会

华为云安全官网

私享会专场用户，优享云安全大礼包，每人1份

欢迎体验华为云安全核心竞争力产品，大礼包价值￥9680，
列表如下：

大礼包内容	适用范围	礼券价值
DDoS高防代金券	高防所有标准套餐	3000元
WAF代金券	WAF所有标准套餐	880元
DBSS代金券	DBSS所有标准套餐	5800元

华为云
技术
私享会

私享会专场用户，优享云安全专属优惠

华为云服务	标准套餐	适用场景	专属优惠政策
DDoS高防	10~30G保底防护套餐	业务初期，非核心竞争业务	6折起售
	≥100G超强防护包年套餐	业务成熟期，核心竞争业务	1折起售 (赠送5~10万按需代金券)
Web应用防火墙	WAF所有标准套餐	所有网站，业务数据敏感	旗舰版5折 其他版6折
数据库安全DBSS	DBSS所有标准套餐	数据库安全合规，防拖库等	高级版5折 专业版6折 基础版7折

华为云
技术
私享会

HUAWEI

HUAWEI

HUAWEI IT大咖说 知识共享平台

华为云
技术
私享会

华为云DDoS高防2.0解决方案

韩宝泽　华为云安全产品总监

华为云全栈防护体系

运营安全

运营管理

- 运营牌照
- 租户生命周期
- 服务生命周期

交易管理

- 责任边界
- 合同管理

租户安全

安全服务

- 自研服务
- 合作生态

云服务安全

- SaaS
- PaaS
- IaaS

基础设施安全

云平台安全

- 数据安全
- 主机安全
- 虚拟网络安全

边界防御安全

- 防火墙
- VPN
- WAF
- IPS
- Anti-DDoS

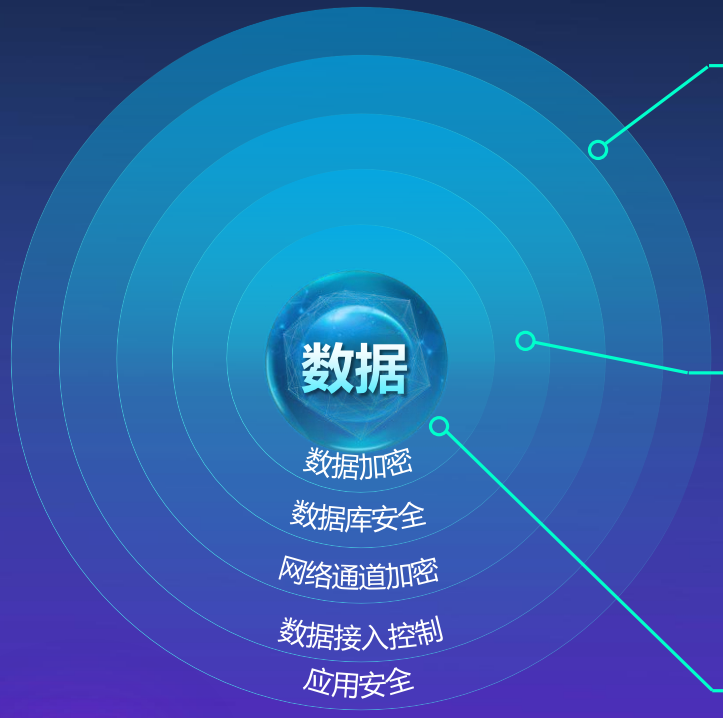
运维安全

- 检测
- 分析
- 感知
- 响应

合规安全（标准和认证）

可信云认证 | 信息安全等保 | ISO27001 | CSA STAR | PCI | SOC | ……

以数据安全为中心，构建的全栈安全服务



安全风险和方案

进不来（应用安全）
- XSS跨站
- 恶意插件
- 木马上传
- 非授权访问
- SQL注入
- 自动学习

看不到（数据库安全）
- 自动发现
- 动态脱敏
- 全面控防
- 精准审计

拿不走（数据加密）
- 密钥管理
- 第三方HSM
- 国际标准算法
- 强合规性

化理念为实践

安全服务

网络安全
- Anti-DDoS
- DDoS高防
- 云防火墙
- 端云协同防护

主机安全
- 资产管理
- 入侵检测
- 漏洞管理
- 基线检查
- 网页防篡改

应用安全
- Web应用防火墙
- Web扫描
- 中间件（含DB）扫描
- 主机扫描
- 弱密码扫描
- 业务逻辑扫描
- 编码扫描

数据安全
- 数据库审计
- 数据脱敏
- 数据库防火墙
- 数据专属加密
- EVS/VBS/IMS/OBS/RDS加密
- 密钥管理
- 密钥对登陆

安全管理
- 态势感知
- 云堡垒机
- 证书管理
- 安全监测
- 主机安全体检
- 网站安全体检
- 应急响应
- 安全加固

DDoS攻击发展趋势

有组织的黑客产业链

- 专业的运作链条
- 成本低
- 难定位

秒级加速，流量更大，更加专业

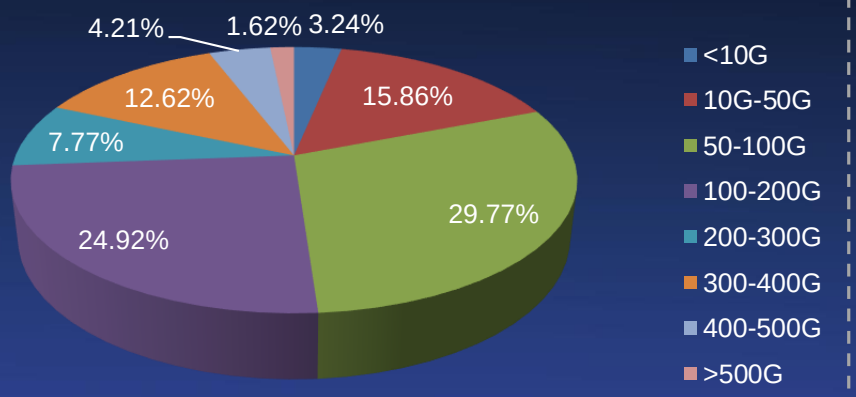
- 攻击流量上升快，几秒即可超百G
- 反射攻击持续升温，不断有新型的开放服务器被挖掘
- 攻击手段越来越专业，混合流量占比高，不断调整攻击手法

IoT终端加入僵尸网络大军

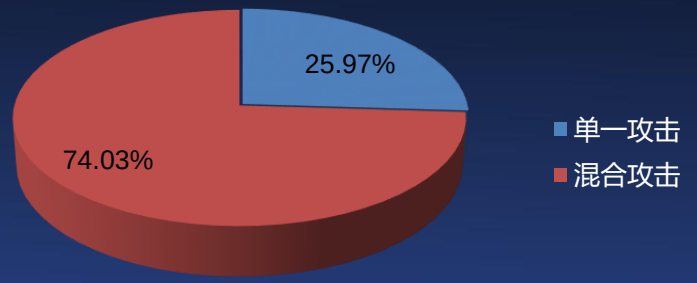
- 安全机制缺失，IoT终端成僵尸网络发展壮大的温床
- 海量IoT僵尸发起T级攻击
- 入侵CCTV摄像头形成僵尸网络，每个摄像头每秒可以发送1到30M数据包

华为云高防2017年DDoS攻击监测数据分析

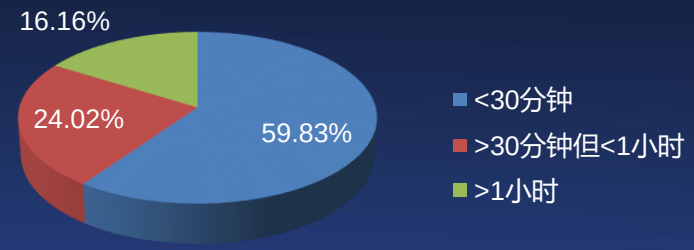
攻击规模量级占比



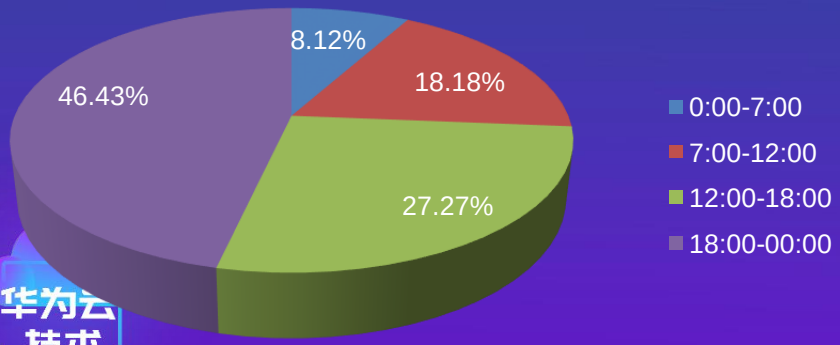
攻击矢量分布



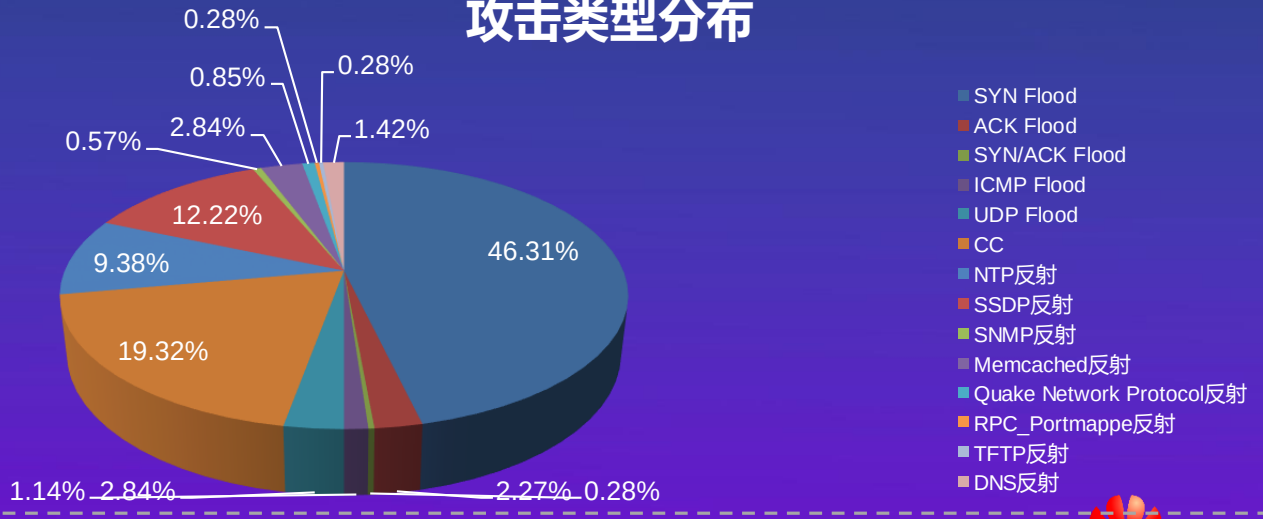
攻击时长占比



攻击发生时间段占比



攻击类型分布

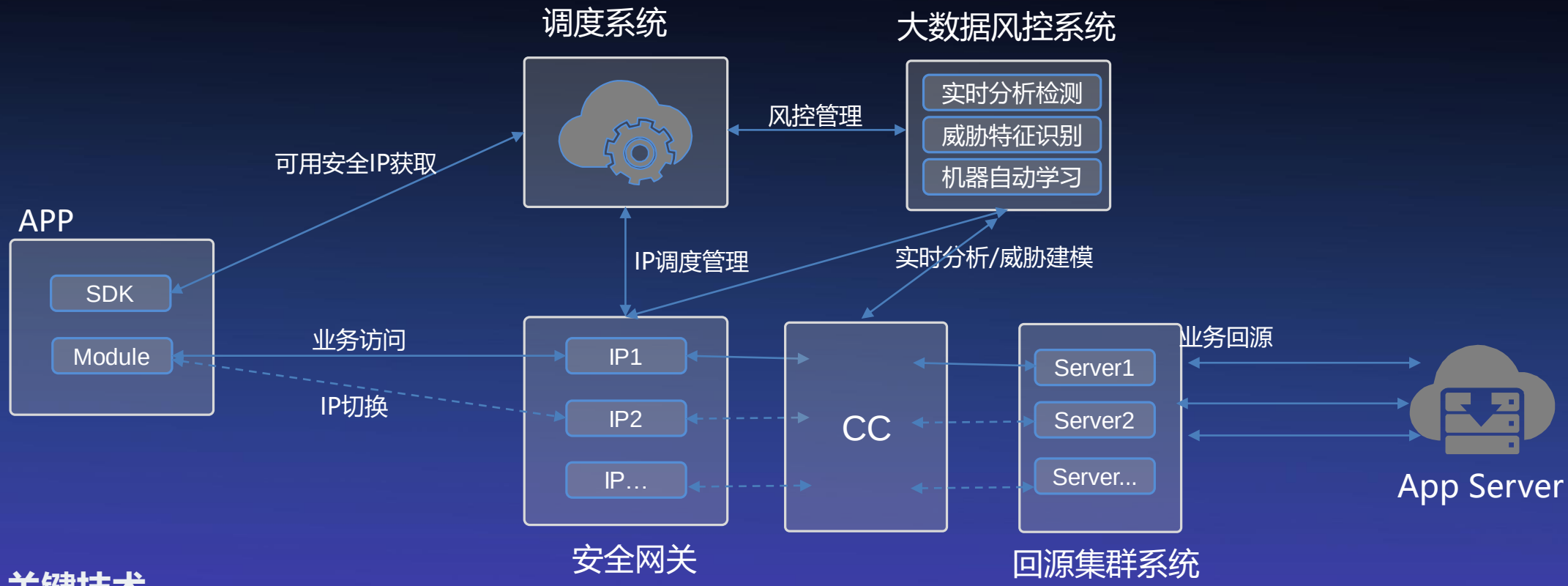


互联网行业为何成为俎上鱼肉

同行竞争激烈，黑客敲诈勒索

- 互联网业务对可用性和连续性要求高，DDOS攻击流失大量用户。游戏协议私有，TCP CC防御难度非常大。攻击成本低，效果好。
- 棋牌类游戏等为迅速抢占市场份额，敏捷快速开发，WEB、APP存在安全漏洞，整体架构存在众多攻击薄弱点。
- 外包或购买开源的代码，无自身技术团队保障，黑客偏爱此类运营商，经不起黑客打击，成为发展重大瓶颈。

高防2.0——端云协同+大数据风控解决方案



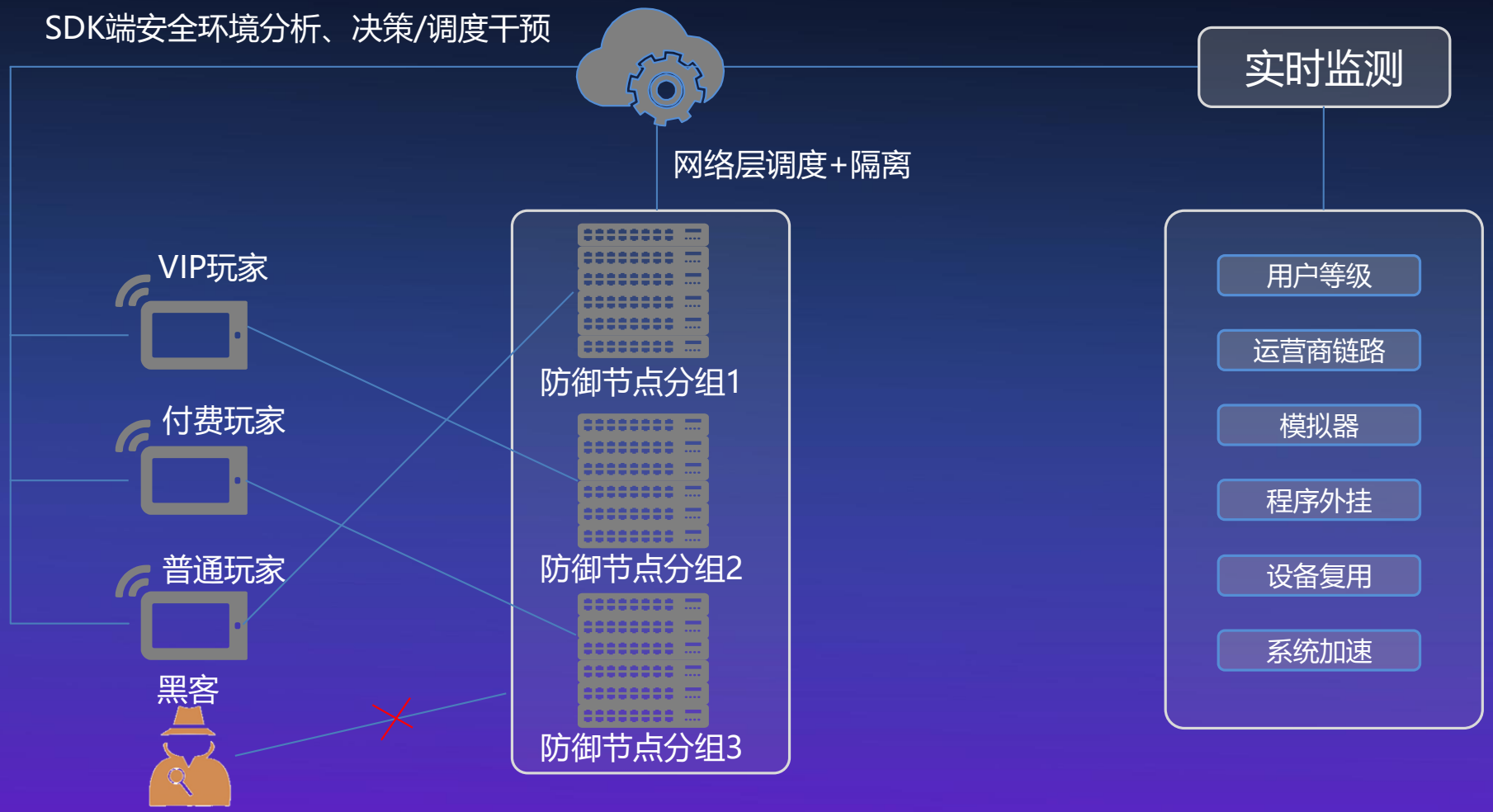
关键技术

智能调度：分组、资源调度

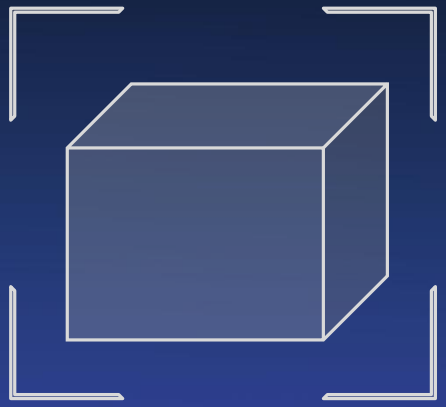
流量染色：加密染色，一人一密/一机一密，防误杀、防破解，正邪一识即破

SDP单包认证：解决APP、端游的CC问题

基于大数据的智能调度，黑客隔离



密钥白盒+流量染色技术，让黑客“显形”



- 动态密钥白盒技术
- 一人一密/一机一密
- 本地/通信数据保护

- 业务逻辑点染色数据
- 染色机制用户可定制
- 流量染色服务侧无改动

全球分布式节点部署，智能优选接入

全球10+清洗节点
带宽储备：10TB
单节点最大防护能力：2TB

（具备无限流量清洗能力）

华为云游戏高防2.0解决方案特点

快速流畅

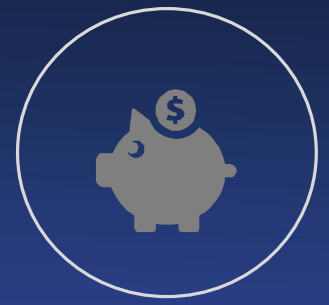
- SDK秒级切换攻击
- 多线BGP高速接入

智能学习

- 业务风控智能隔离
- 黑客攻击机器学习

精准防护

- 流量染色技术
- SDP认证技术



高性价比

- 无限攻击防御能力
- 定制方案成本可控

THANK YOU

HUAWEI

HUAWEI IT大咖说 知识共享平台

华为云 技术 私享会

网络安全等级保护定级指引

龙军　　深圳市网安计算机安全检测技术有限公司

主要内容

核心观点

等级保护测评是国家强制的合规性检查

等级保护的目的是加强信息系统的安全防范能力

等级保护过程是系统安全能力完善的过程

等级保护是企业信息安全宣传的有利证明

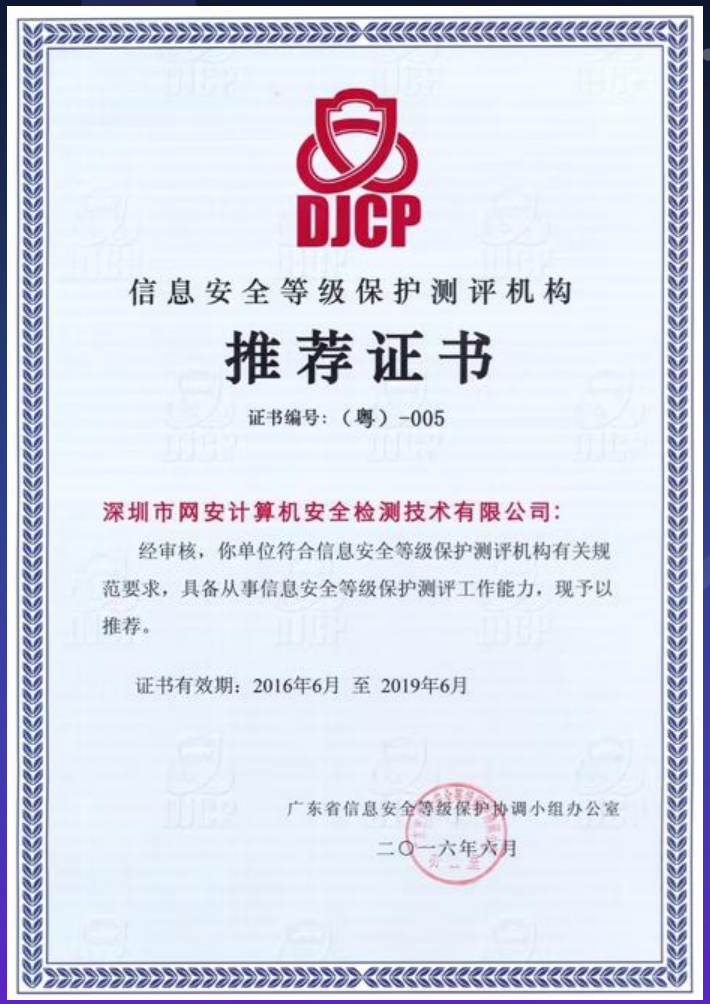
核心优势

- 我公司是最早参与等级保护评测的机构之一
- 我公司是迄今为止全国等保测评机构中测评量最高的机构
- 我公司在等保测评方面经验极其丰富
- 我们和等保政策和标准制定单位有良好的沟通
- 我公司和监管机构有良好的合作关系
- 我公司可提供等保系列和信息系统安全运维的全面服务

网安公司简介

网安公司是公安部授权的等级测评机构，同时拥有广东省公安厅认可的安全服务资质。

网安公司也是深圳地区唯一具有等级测评资质的第三方商业机构，拥有一支由博士后、博士带队的经验丰富、理论知识深厚的测评队伍，每年为超过400家单位和机构的近1000个信息系统提供等级测评服务，测评质量得到了等级保护主管机构和广大客户的高度认可。



DJCP

信息安全等级保护测评机构

推荐证书

证书编号：（粤）-005

深圳市网安计算机安全检测技术有限公司：

经审核，你单位符合信息安全等级保护测评机构有关规范要求，具备从事信息安全等级保护测评工作能力，现予以推荐。

证书有效期：2016年6月 至 2019年6月

广东省信息安全等级保护协调小组办公室

二〇一六年六月

深圳市信息安全等级保护测评机构

信息安全等级保护测评机构是指具备本规范的基本条件，经能力评估和审核，由**省级以上信息安全等级保护工作协调（领导）小组办公室**推荐，从事等级测评工作的机构。

等级保护工作流程

系统定级	• **经营使用单位**、行业主管单位
系统备案	• **经营使用单位**、公安机关
建设整改	• **经营使用单位**
等级测评	• **经营使用单位**、**测评机构**
监督检查	• 国家监管部门、公安机关、行业主管单位

等级保护测评目标

测评目标

通过对信息系统的安全测评来评判目前信息系统安全保护的程度或水平与国家信息系统安全等级保护要求之间的差距，以便指导对信息系统进行安全方面的调整和改进，确保信息系统的安全防护水平达到国家信息系统安全等级保护的要求。

等级保护制度的主要内容

核心内容

国家制定统一的政策，各单位、各部门依法开展等级保护工作。实行信息安全等级保护，是在信息安全保障工作中国家意志的体现，具有明显的强制性。同时，坚持“自主定级”、“自行建设”、“自主保护”，体现了“谁主管、谁负责，谁使用、谁负责，谁运营、谁负责”的信息安全责任制。

主要内容

一、网络安全等级保护测评介绍

二、定级备案-背景

三、定级备案-系统分类分级

四、等级测评-测评实施

二、定级备案-法律依据

第二十一条 国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：

（一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；

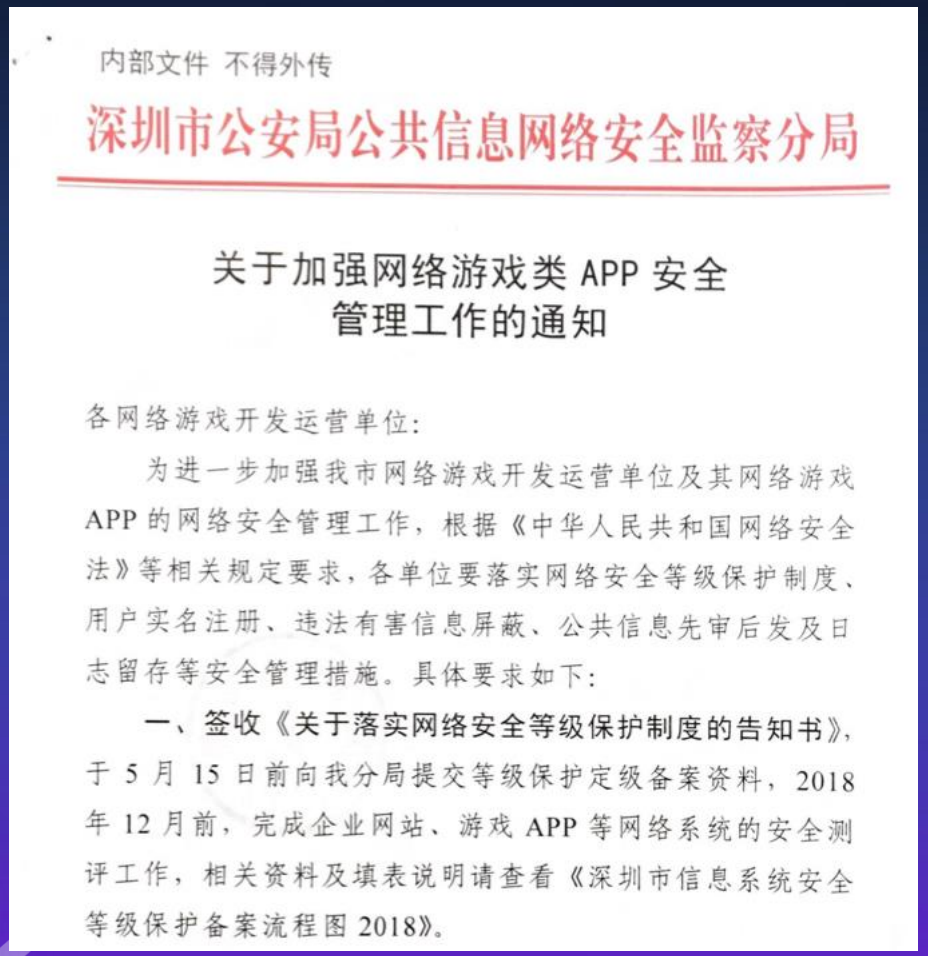
（二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；

（三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；

（四）采取数据分类、重要数据备份和加密等措施；

（五）法律、行政法规规定的其他义务。

二、定级备案-政策要求



内部文件 不得外传

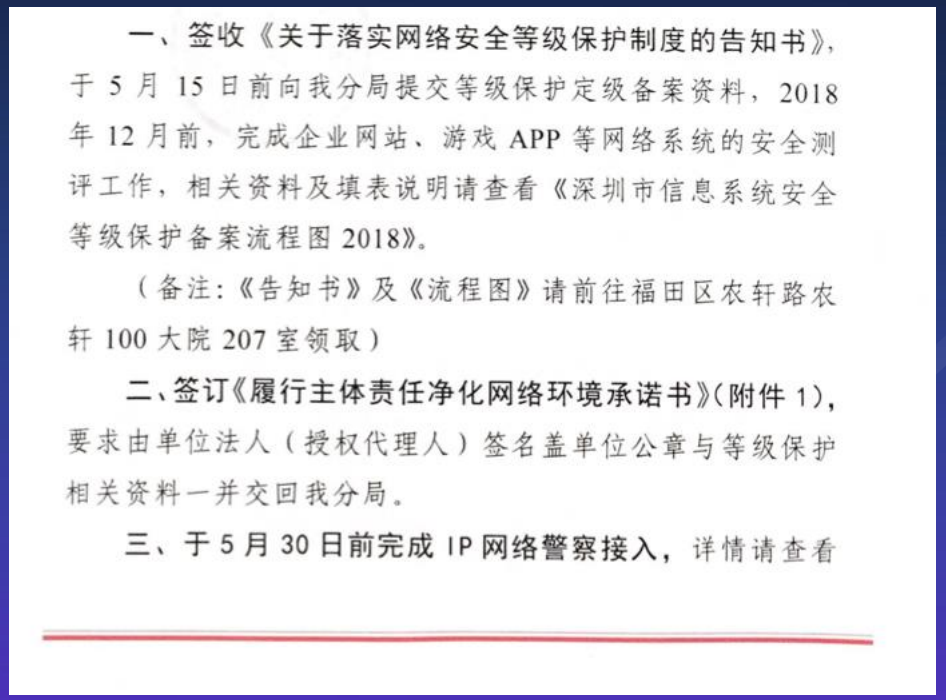
深圳市公安局公共信息网络安全监察分局

关于加强网络游戏类 APP 安全管理工作的通知

各网络游戏开发运营单位：

为进一步加强我市网络游戏开发运营单位及其网络游戏APP的网络安全管理工作，根据《中华人民共和国网络安全法》等相关规定要求，各单位要落实网络安全等级保护制度、用户实名注册、违法有害信息屏蔽、公共信息先审后发及日志留存等安全管理措施。具体要求如下：

一、签收《关于落实网络安全等级保护制度的告知书》，于5月15日前向我分局提交等级保护定级备案资料，2018年12月前，完成企业网站、游戏APP等网络系统的安全测评工作，相关资料及填表说明请查看《深圳市信息系统安全等级保护备案流程图2018》。



一、签收《关于落实网络安全等级保护制度的告知书》，于5月15日前向我分局提交等级保护定级备案资料，2018年12月前，完成企业网站、游戏APP等网络系统的安全测评工作，相关资料及填表说明请查看《深圳市信息系统安全等级保护备案流程图2018》。

（备注：《告知书》及《流程图》请前往福田区农轩路农轩100大院207室领取）

二、签订《履行主体责任净化网络环境承诺书》（附件1），要求由单位法人（授权代理人）签名盖单位公章与等级保护相关资料一并交回我分局。

三、于5月30日前完成IP网络警察接入，详情请查看

二、定级备案-受侵害的客体

等级保护对象受到破坏时所侵害的客体包括以下三个方面：

a) 公民、法人和其他组织的合法权益；
b) 社会秩序、公共利益；
c) 国家安全。

侵害社会秩序的事项包括以下方面：

影响国家机关社会管理和公共服务的工作秩序；
影响各种类型的经济活动秩序；
影响各行业的科研、生产秩序；
影响公众在法律约束和道德规范下的正常生活秩序等；
其他影响社会秩序的事项。

侵害公共利益的事项包括以下方面：

影响社会成员使用公共设施；
影响社会成员获取公开信息资源；
影响社会成员接受公共服务等方面；
其他影响公共利益的事项。

侵害公民、法人和其他组织的合法权益：

是指由法律确认的并受法律保护的公民、法人和其他组织所 享有的一定的社会权利和利益等受到损害。

二、定级备案-侵害程度

等级保护对象受到破坏后对客体造成侵害的程度归结为以下三种:

a) 造成一般损害;
b) 造成严重损害;
c) 造成特别严重损害。

一般损害:
工作职能受到局部影响,业务能力有所降低但不影响主要功能的执行,出现较轻的法律问题,较低的财产损失,有限的社会不良影响,对其他组织和个人造成较低损害 。

严重损害 :
工作职能受到严重影响,业务能力显著下降且严重影响主要功能执行,出现较严重的法律问题,较高的财产损失,较大范围的社会不良影响,对其他组织和个人造成较严重损害 。

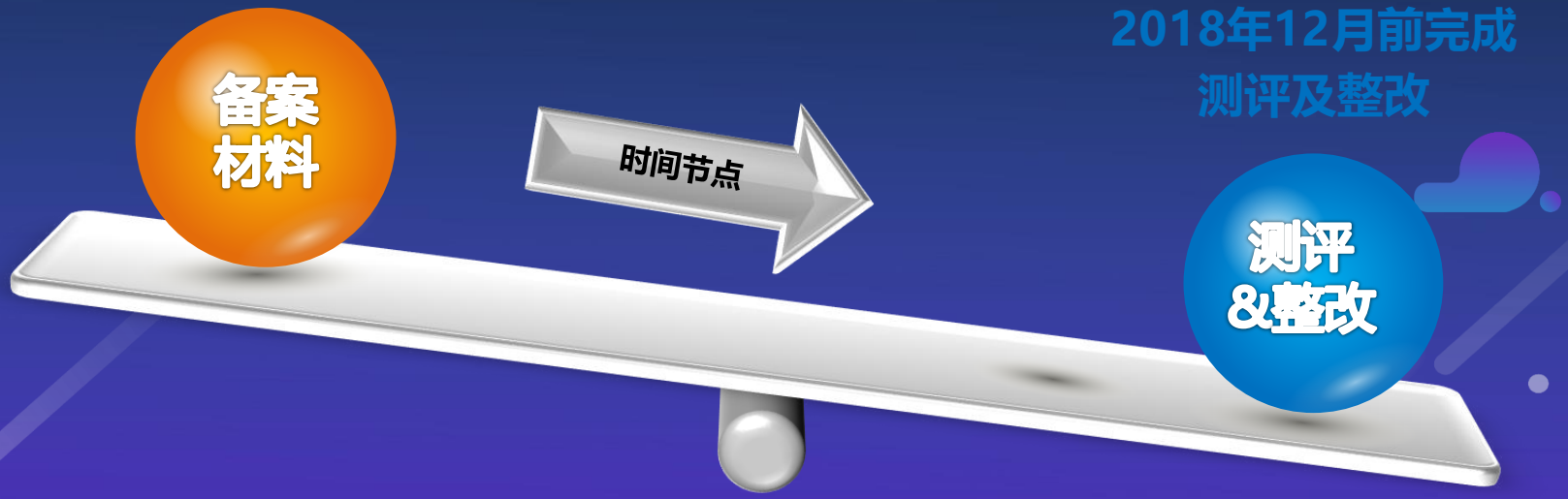
特别严重损害:
工作职能受到特别严重影响或丧失行使能力,业务能力严重下降且或功能无法执行,出现极其严重的法律问题,极高的财产损失,大范围的社会不良影响,对其他组织和个人造成 非常严重损害 。

二、定级备案-定级指南要求

受侵害的客体	对客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第三级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

二、定级备案-时间节点

2018年5月15日提交
备案材料



2018年12月前完成
测评及整改

二、定级备案-定级要求

备案：

根据《信息安全等级保护管理办法》，信息系统安全保护等级为第二级以上的信息系统运营使用单位或主管部门，应当在安全保护等级确定后30日内，到当地公安机关网监部门办理备案手续。新建第二级以上信息系统，应当在投入运行后30日内，由其运营、使用单位到当地公安机关网监部门办理备案手续。

主要内容

一、网络安全等级保护测评介绍

二、定级备案-背景

三、定级备案-系统分类分级

四、等级测评 - 测评实施

三、定级备案-系统分类

游戏系统分类分级

表1 网络游戏开发运营单位信息系统定级建议

序号	信息系统	建议安全保护等级			
		实名用户数量不足三十万级	实名用户数量达到三十万级	自有支付系统	纯宣传类
1	门户网站系统	-	-	-	第二级
2	用户管理系统认证计费系统	第二级	第三级	第三级	-
3	游戏论坛、社区等交互系统	第二级	第三级	-	-
4	战网类游戏平台	第二级	第三级	第三级	-
5	游戏信息系统	第二级	第三级	第三级	-

三、定级备案-定级对象

游戏系统定级对象

表2 定级对象

分类	信息系统用途
门户网站类	网络游戏企业门户网站、游戏宣传门户。
用户管理系统	提供用户注册、用户实名认证，以及为下属所运营游戏提供统一用户认证。提供用户充值。
游戏论坛及社区	为玩家提供的游戏类讨论与经验分享讨论。
战网类游戏平台	为旗下多款游戏提供统一入口和用户认证的游戏平台，如 QQ 游戏大厅等。
游戏信息系统	角色扮演类、动作类、棋牌类、射击类等等游戏信息系统，其中包涵 APP（安卓、IOS）应用（游戏业务应用 APP 需要做安全检测、安全加固。）

主要内容

一、网络安全等级保护测评介绍

二、定级备案-背景

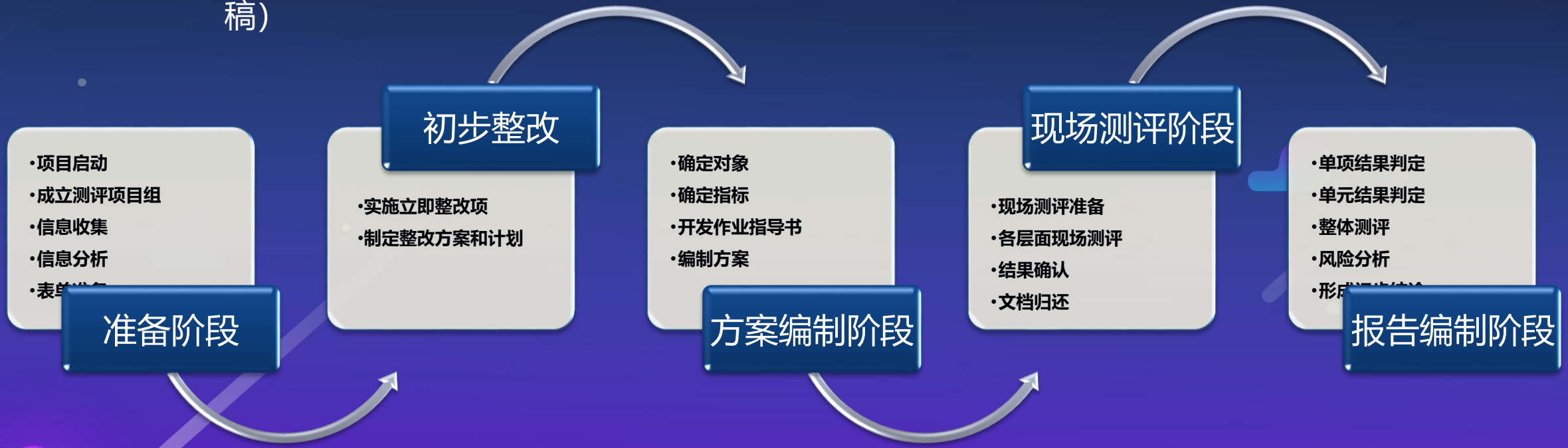
三、定级备案-系统分类分级

四、等级测评-测评实施

华为云
技术
私享会

四、等级测评-项目流程

- 《信息安全技术 网络安全等级保护基本要求》（GB/T 22239—20XX）（征求意见稿）
- 《信息安全技术 网络安全等级保护测评要求》（GB/T 28448—20XX）（征求意见稿）



四、等级测评-三级测评内容

网络安全等级保护第三级基本要求					
安全管理-37控制点-115要求项			安全技术-34控制点-115要求项		
安全策略和管理制度	4控制点	7要求项	物理和环境安全	10控制点	22要求项
安全管理机构和人员	9控制点	26要求项	网络和通信安全	8控制点	33要求项
安全建设管理	10控制点	34要求项	设备和计算安全	6控制点	26要求项
系统运维管理	14控制点	48要求项	应用和数据安全	10控制点	34要求项
71个控制点，230个检查项					

四、等级测评-二级测评内容

网络安全等级保护第二级基本要求					
安全管理-37控制点-76要求项			安全技术-31控制点-69要求项		
安全策略和管理制度	4控制点	6要求项	物理和环境安全	10控制点	15要求项
安全管理机构和人员	9控制点	16要求项	网络和通信安全	6控制点	15要求项
安全建设管理	10控制点	23要求项	设备和计算安全	6控制点	17要求项
系统运维管理	14控制点	31要求项	应用和数据安全	9控制点	22要求项
68个控制点，145个检查项					

等级保护测评结论

测评结论	判别依据
符合（100分）	等级测评结果中不存在部分符合项或不符合项
基本符合（75~99）	等级测评结果中存在部分符合项或不符合项，但不会导致信息系统面临高等级安全风险
不符合（1~75）	等级测评结果中存在部分符合项或不符合项，导致信息系统面临高等级安全风险

THANK YOU

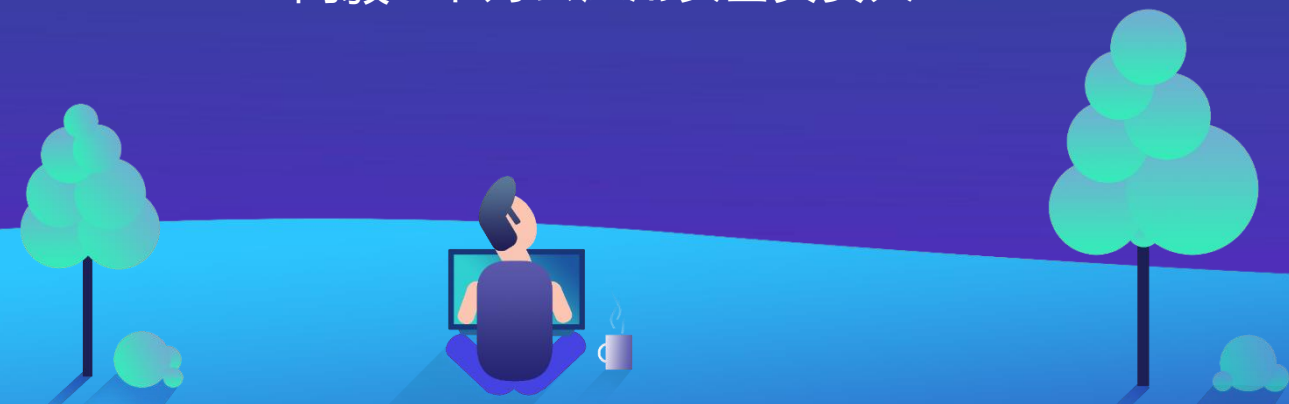
HUAWEI

HUAWEI IT大咖说 知识共享平台

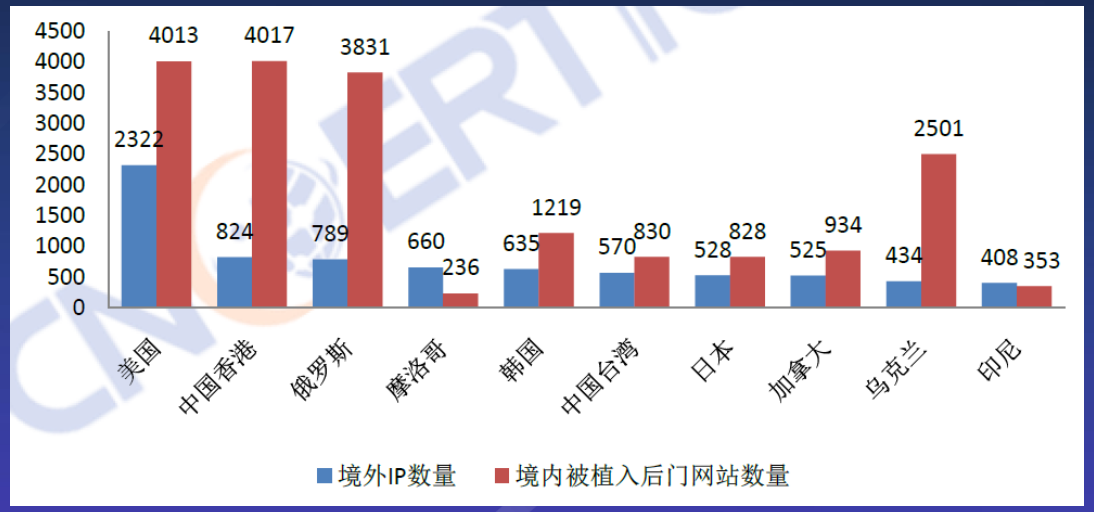
华为云
技术
私享会

华为云游戏网站Web防护方案

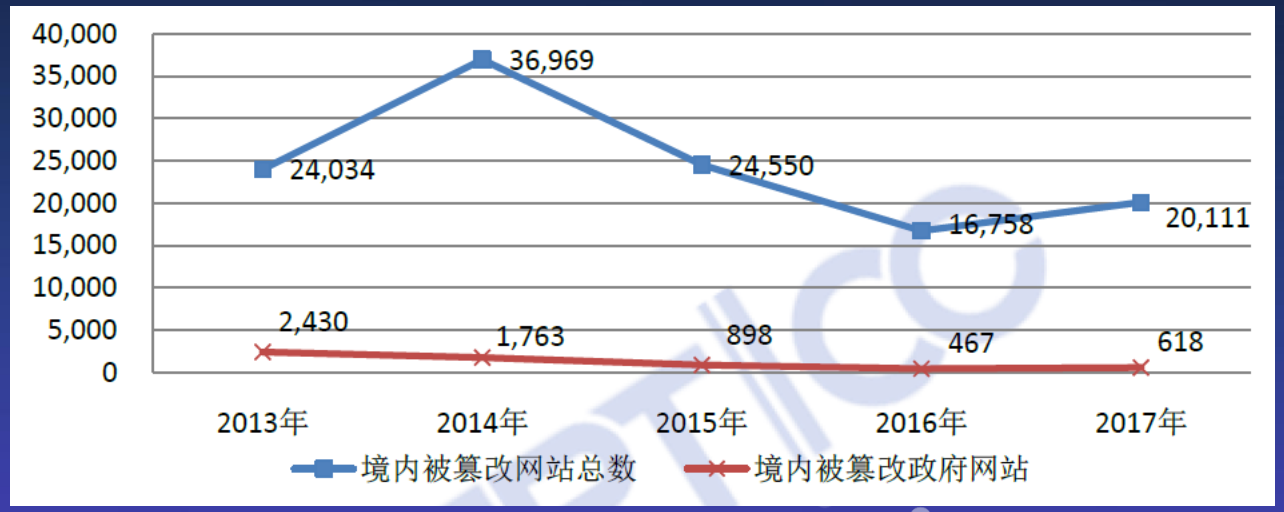
高毅　华为云应用安全负责人



中国互联网Web安全现状



2017年境外向我国境内网站植入后门IP地址所属国家或地区TOP10



2013 - 2017年我国境内被篡改网站数量情况

数据来源：国家互联网应急中心《2017年我国互联网网络安全态势综述》

游戏行业Web安全事件

A游戏官网游戏入口被篡改B游戏

2017年10月，某游戏官网被黑客植入非法内容

2018年2月，某游戏网站因泄漏用户数据导致大量账号被盗

Web应用防火墙，专为Web安全而生

基于业务属性，配置针对性的安全策略

通过漏洞扫描服务，发现潜在漏洞

事前准备

扫描、探测行为的拦截

注入、跨站等OWASP 10攻击行为拦截

0day威胁防御

CC攻击的精准防护

事中防御

爬虫、自动化软件的拦截

Web应用防火墙

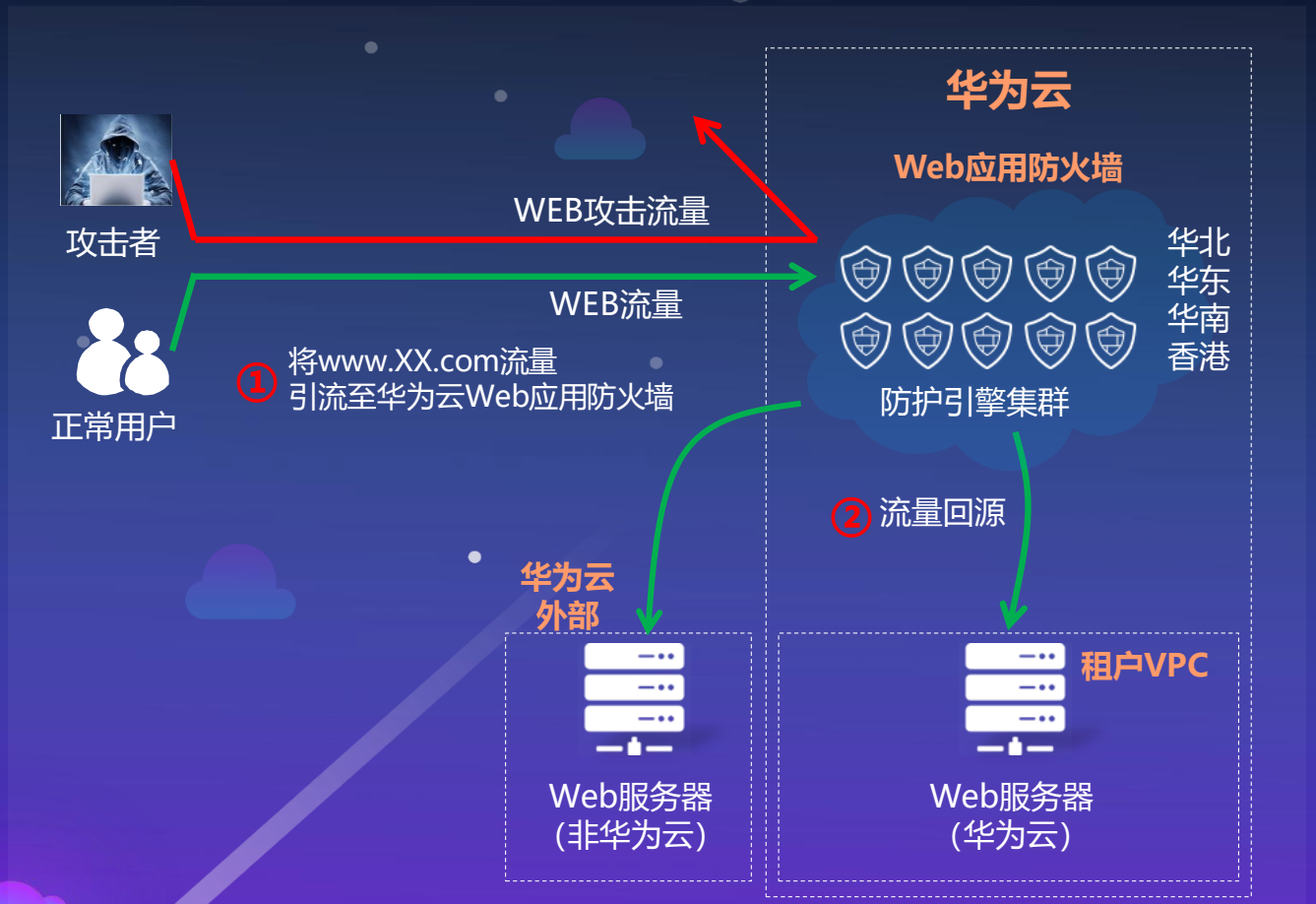
事后审计

输出丰富的安全态势

输出详细的安全事件

华为云技术私享会

华为云WAF，Web服务的“最佳搭档”



“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。” ——Gartner 2017

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双重验证阻断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

三引擎架构，威胁检出率提升30%以上

正则引擎

防御OWASP通用攻击

语义引擎

高效防护XSS/SQL注入攻击

AI引擎

防御高级威胁/0day等攻击

领先的动态防爬虫算法，有效防止数据泄露

JS JavaScript解析

浏览器指纹

加密验证技术

三管齐下，精准识别&防御CC攻击

基于IP

根据IP地址识别客户端

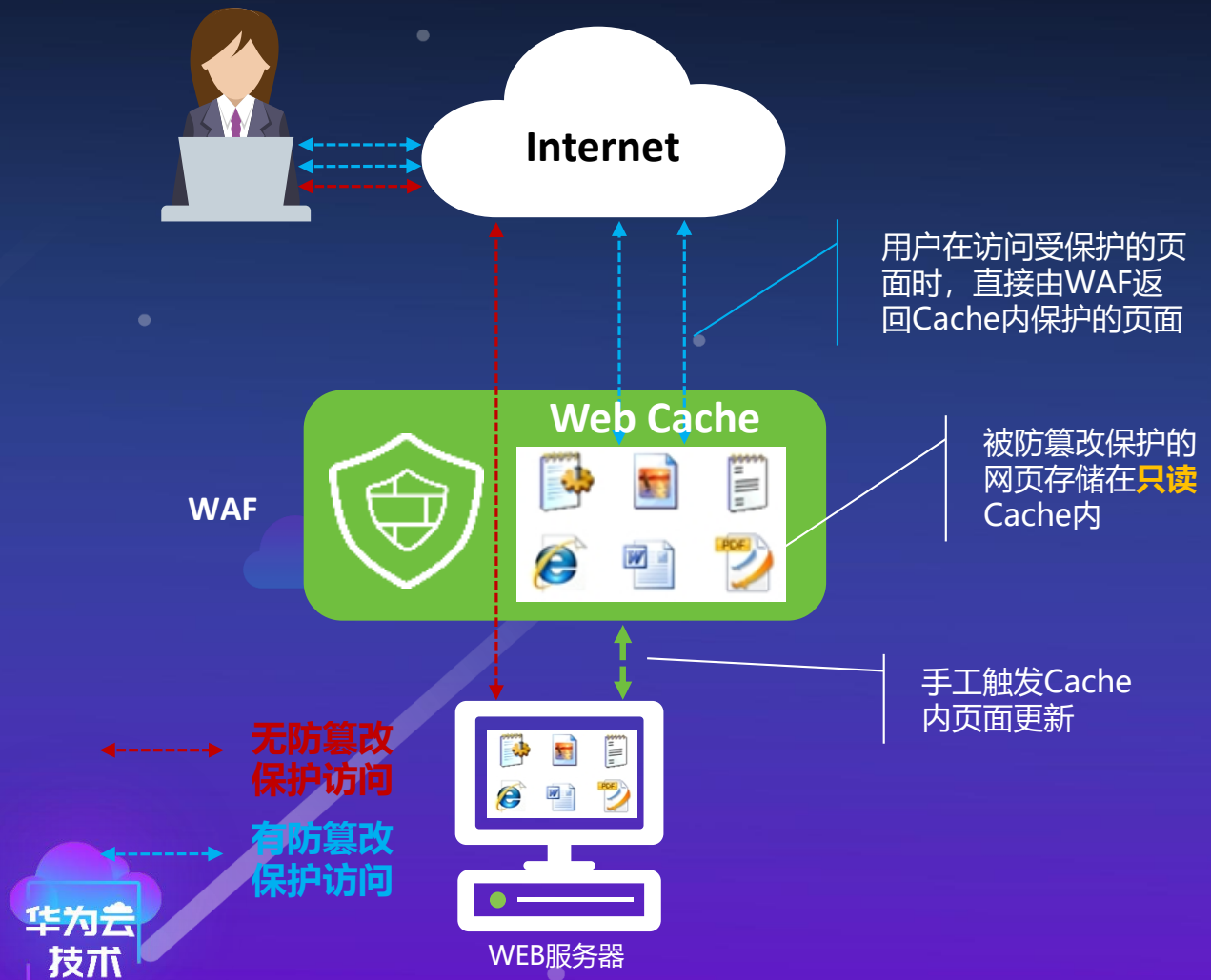
基于Cookie

根据Cookie字段识别客户端

基于AI

利用AI技术实现“人机识别”

多重防护机制，有效阻止网页被篡改



挂马检测

从源头上阻断网页被篡改

Web Cache机制

缓存网页，“视觉”防篡改

健康状态监测

监控网页健康状态，实时告警

AI引擎，智能推荐防御规则

场景	AI引擎
黑名单	自动识别有恶意行为的IP，并推荐给用户进行拦截。
CSRF防护	自动找出经常被盗链的页面（URI），并自动识别正常情况下的上一跳，推荐Referer字段
恶意爬虫	识别有爬虫行为的IP，找出对应特征（如IP、UA），并推荐给用户进行拦截
隐私防护	自动识别具有用户名、密码、用户地址等敏感信息的页面
误报检测	自动分析用户所选的误报条目，总结误报原因，向用户推荐白名单策略
CC攻击	对不同的页面，不同的客户端IP，自动分析出总访问次数门限值和各个IP访问次数门限值
WebShell	根据页面之间的链接关系和用户访问频次识别出WebShell页面

专业可靠，源于华为安全的16年积累

稳定可靠

冗余保障、异地容灾

专业易用

规则库实时更新、0day漏洞修补

隐私保护

华为“三不”原则

华为云
技术
私享会

深圳某游戏公司的Web防护方案

客户介绍

XX游戏是中国领先的互联网游戏开发和运营商，致力于多元化的网络游戏开发、运营和授权代理，拥有优秀的研发、发行团队，并不断更新技术和理念，一直在行业内保持着领先地位。

解决方案

为XX游戏提供DDoS高防、Web应用防火墙等**弹性**安全服务。

客户价值

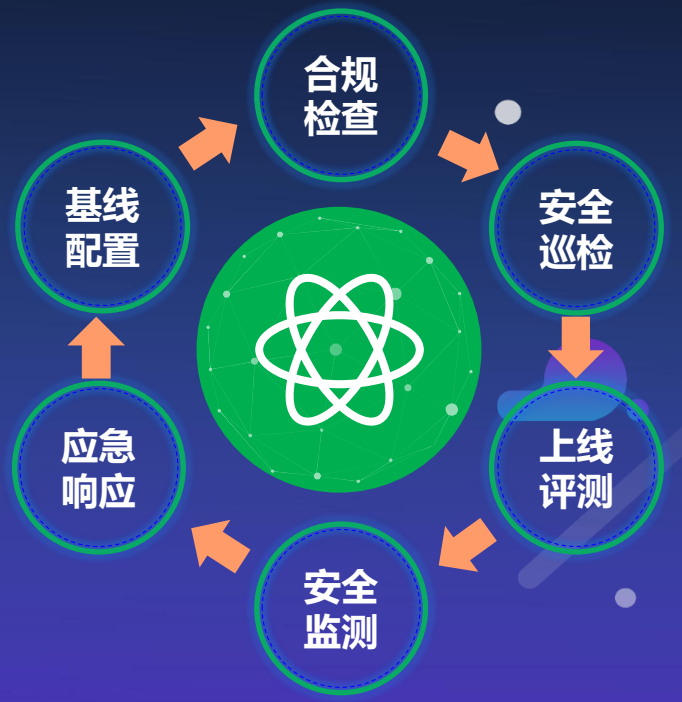
在WAF上线以来，平均每天成功抵御数万次的Web攻击，为XX游戏的在线业务和在线交易保驾护航。WAF灵活的弹性架构可以很好的满足XX游戏当前和未来的业务需求。

漏洞扫描服务全面升级，覆盖业务全生命周期

全面升级

开发阶段

（安全）运维阶段



漏洞扫描服务

- 编码安全性检查
- 主机扫描
- Web扫描
- 逻辑扫描
- 数据库扫描
- 安全基线
- 弱口令
- 中间件扫描

华为云技术私享会

THANK YOU

HUAWEI

HUAWEI IT大咖说 知识共享平台

华为云
技术
私享会

云上数据库一体化保险箱

——华为云数据库安全服务

刘洪善　华为云安全产品总监，品牌与运营负责人

数据库安全客户关注点1：等保合规

【第二十一条】 国家实行网络安全等级保护制度。网络运营者应当按照**网络安全等级保护制度**的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：

- （一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；
- （二）采取防范计算机病毒和**网络攻击、网络侵入**等危害网络安全行为的技术措施；
- （三）采取**监测、记录网络运行状态、网络安全事件的技术**措施，并按照规定留存相关的网络日志不少于六个月；
- （四）采取**数据分类、重要数据备份和加密**等措施；
- （五）法律、行政法规规定的其他义务。

- **解读：**
- （二）本条要求采取防范网络入侵的措施。对数据库而言，可采用数据库防火墙，保护数据库不被入侵
- （三）本条要求监测运安全事件。对数据库而言，可采用数据库监控和审计，对攻击行为进行记录；且日志的存储期限不低于6个月。
- 法律责任：第五十九条：（警告）->（1~10万罚款）
- 责任人：5千~5万罚款
- 此外，在【第二十五条：应急预案】，【第二十八条：配合协助】，【第四十二条：个人信息保护】等也有类似要求。

游戏 | 狭义政府 电子政务 公共服务 | 三甲医院 | 互联网金融 信用社 证券公司 | 普教 高校 | 科研型企业 | 电力公司 | 轨道交通 | …

数据库安全客户关注点2：敏感数据泄露

敏感数据来源于哪里

数据泄露的主要途径

1. 黑客攻击：SQL注入，脱库撞库，高级持续性威胁，弱口令扫描等
2. 内部人员泄露：滥用和恶意使用云服务，内外串通等
3. 第三方集成商/开发商：数据未加密/脱敏，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等

数据脱敏是防止数据泄漏的主要方法

脱敏所有：所有数据都被脱敏。

空：以空字符串返回。

信用卡脱敏：显示信用卡的最后四位数字，其他字符被脱敏。

显示随机数：显示随机数而不是原始数据。

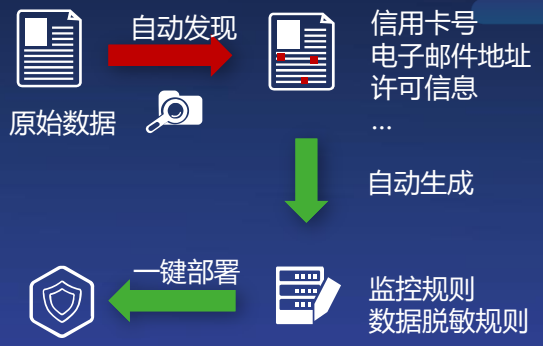
全邮箱脱敏：电子邮件地址的用户名和域都被脱敏。例如： ‘abcdefg@company.com’ 转换为 ‘XXXXXXX@XXXXXXX.com’

隐藏所有数字：脱敏字符串中的所有数字。例如：邮政编码中的所有数字都被脱敏如下： ‘123456’ 转换为 ‘******’

固定字符串：用 ‘CONFIDENTIAL’ 替换列中的所有值

事前：数据库中针对数据泄露保护的几个设计

敏感数据发现



- ✓ 根据合规要求**自动发现**敏感数据，一键进行合规检查
- ✓ 根据发现结果**自动生成**规则，降低运维复杂度
- ✓ 用户**自定义正则表达式**，满足特定场景数据发现要求
- ✓ 用户**自定义发现频率**，可定期检查持续改进

数据动态脱敏

- ✓ **细粒度脱敏**，实现行级、列级、表级、视图级脱敏，以及按指定条件脱敏
- ✓ **高性能**的数据动态脱敏，不影响数据库和应用，非生产应用访问生产数据时数据不泄露

法律合规遵从

PCI DSS 第三方支付行业数据安全标准

HIPAA 美国医疗行业合规法案

Sarbanes-Oxley Act 塞班斯法案

- ✓ 内置PCI-DSS、HIPAA、SOX等**合规知识库**，满足国际企业合规要求
- ✓ **自定义合规**规则
- ✓ 生成友好的遵从**合规报告**，方便审计

华为云技术私享会

示例：敏感数据发现的配置和结果呈现

- 某个金融客户数据库中有员工敏感数据。
- 数据库被黑客攻破以后，将敏感数据全盗取。

```
mysql> select * from workmates;
+----+-----------+-----+---------+------------+-----+--------------------+------------------+
| id | name      | sex | addr    | birth      | age | email              | creditcard       |
+----+-----------+-----+---------+------------+-----+--------------------+------------------+
|  1 | Guojing   | m   | Shaanxi | 1988-04-28 |  29 | guojing@gmail.com  | 6222222222222222 |
|  2 | Yangguo   | m   | Hubei   | 1987-12-01 |  30 | yangkang@qq.com    | 6333333333333333 |
|  3 | Huangrong | f   | Zhejiang| 1988-08-15 |  29 | huangrong@126.com  | 6444444444444444 |
|  4 | Lilei     | m   | Beijing | 1977-05-21 |  40 | lilei@gmail.com    | 6555555555555555 |
|  5 | Han       | f   | Xinjiang| 1978-01-05 |  39 | hanmeimei@163.com  | 6666666666666666 |
+----+-----------+-----+---------+------------+-----+--------------------+------------------+
5 rows in set (0.00 sec)
```

- 用户使用敏感数据发现功能：发现了敏感字段。客户选择了一键生成脱敏规则。

表	列	匹配类型	合规	级别	扫描行数	匹配结果	监控规则	脱敏规则
confidential.workmates	email	E-Mail	HIPAA	suspected	6	100%	☐	☑
confidential.workmates	creditcard	regex-sample	GROUP-SAMPLE	sensitive	6	17%	☐	☑

生成

示例：敏感数据发现的配置和结果呈现

- 客户选择一键生成了脱敏规则

成功创建2条脱敏规则

> 显示执行信息

CSV

表	列	匹配类型	合规	级别	扫描行数	匹配结果	监控规则	脱敏规则
confidential.workmates	email	E-Mail	HIPAA	suspected	6	100%	☐	☑
confidential.workmates	creditcard	regex-sample	GROUP-SAMPLE	sensitive	6	17%	☐	☑

- 黑客再次查询的时候，就发现敏感数据被脱敏了：

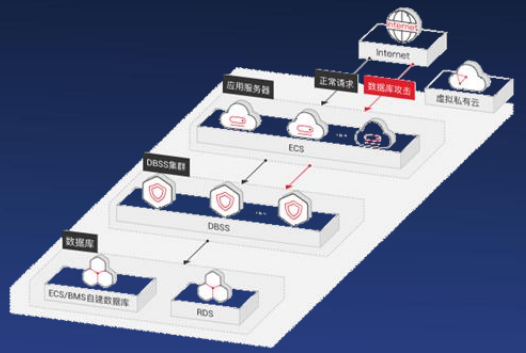
```
mysql> select * from workmates;
+----+-----------+-----+----------+------------+-----+--------------------+--------------------+
| id | name      | sex | addr     | birth      | age | email              | creditcard         |
+----+-----------+-----+----------+------------+-----+--------------------+--------------------+
|  1 | Guojing   | m   | Shaanxi  | 1988-04-28 |  29 | XXXXXXXXXXXXXXXXX  | XXXXXXXXXXXXXXXXX  |
|  2 | Yangguo   | m   | Hubei    | 1987-12-01 |  30 | XXXXXXXXXXXXXXX    | XXXXXXXXXXXXXXXXX  |
|  3 | Huangrong | f   | Zhejiang | 1988-08-15 |  29 | XXXXXXXXXXXXXXXXX  | XXXXXXXXXXXXXXXXX  |
|  4 | Lilei     | m   | Beijing  | 1977-05-21 |  40 | XXXXXXXXXXXXXXX    | XXXXXXXXXXXXXXXXX  |
|  5 | Han       | f   | Xinjiang | 1978-01-05 |  39 | XXXXXXXXXXXXXXXXX  | XXXXXXXXXXXXXXXXX  |
+----+-----------+-----+----------+------------+-----+--------------------+--------------------+
5 rows in set (0.04 sec)
```

事中：数据库防火墙对于非法访问和入侵的防御设计

细粒度访问控制

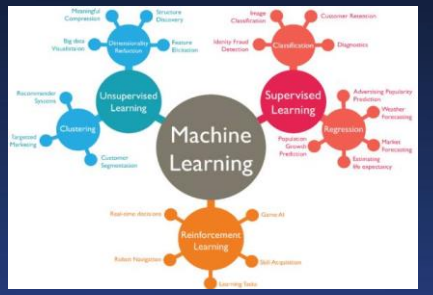
- ✓ **基于角色的访问控制**，如：
  - 查询者分配只读权限
  - DBA只分配创建权限，不分配读权限
- ✓ **最小权限分配原则**，实现客户化定义，谁在什么时间允许干什么
- ✓ **细粒度管控，**可以到表、行、列、事件等

数据库入侵防御



- ✓ **内置知识库**，基于攻防经验的入侵检测、防御
- ✓ **SQL注入攻击防御，**可疑或者危险的查询无法到达数据库
- ✓ 针对特定安全等级**设置门槛值**
- ✓ 可以整合业界**攻击特征库**，减少误报率

规则自学习



- ✓ **机器学习能力**，定期自我学习，生成安全模式规则，应用到数据库防火墙策略中
- ✓ 学习后的规则**可直接**应用于生产环境
- ✓ 可创建查询组，作为防火墙策略的**有效模式规则**（白名单）或者作为一个**不被允许的模式**（黑名单）

示例：数据库防火墙的策略定义和效果呈现

- 客户近期发现数据库的数据频频收到注入攻击。
- 注入的攻击最后呈现的语句如下：

```
mysql> select * from userinfo where name='' or '1'='1' and passwd = '' or '1'='1';
+----+-----------+---------------+---------+
| id | name      | passwd        | comment |
+----+-----------+---------------+---------+
|  1 | 郭靖      | Guojing@12    | NULL    |
|  2 | 黄蓉      | Huangrong@12  | NULL    |
|  3 | 洪七公    | Hongqigong@12 | NULL    |
|  4 | 风清扬    | Shuaige@12    | NULL    |
+----+-----------+---------------+---------+
4 rows in set (0.06 sec)
```

- 客户决定使用数据库防火墙，
- 并配置SQL注入防护规则。

示例：数据库防火墙的策略定义和效果呈现

- 防护之后，客户发现数据库侧的SQL注入攻击已经没了。

```
mysql> select * from userinfo where name='' or '1'='1' and passwd = '' or '1'='1';
ERROR 1045 (HY000): ACCESS DENIED
mysql>
```

- 同时在管理页面发现有SQL入侵日志。

事件ID	#1	规则ID	#2
日期	2018-05-03 17:30:45	规则类型	Risk Based - IPS/IDS
动作	阻止	SQL注入	55
风险结果	该条查询具有OR token。 检测到真表达式（SQL重言式）。 该条查询含有空的密码表达。		
动作原因	风险计算		
模式	select * from userinfo where name = ? or ? = ? and passwd = ? or ? = ?		
原查询	select * from userinfo where name='' or '1'='1' and passwd = '' or '1'='1'		

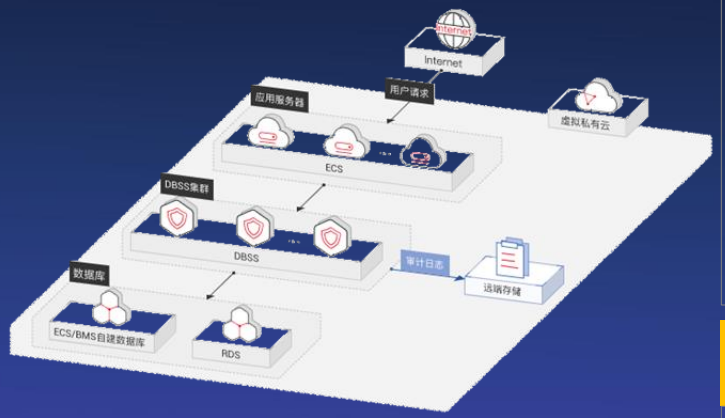
事后：用数据库审计技术来对黑客行为进行震慑

异常监控

- **行为异常监控：**
  ①提供登录行为异常监控； ②列级、表级、存储过程级别的访问异常监控 ③提供管理员权限准入异常监控等
- **数据异常监控：** 提供原始数据修改标识，包括源IP地址、用户、应用名称、受影响的行、修改时间等信息
- **性能异常监控：** 提供CPU、内存、网络流量等资源监控能力

日志记录

- **记录流量日志**
- **记录入侵日志**
- **记录异常监控日志**
- **记录数据脱敏日志**
- **远程日志能力**



报告审计

- **PII事前事后的审计**
- **内置入侵检测报告**，包括入侵IP、入侵用户、阻止的应用程序、阻止的查询和错误登录源等信息
- **针对普通用户的审计**，包括用户设置、用户访问权限、非活跃用户、密码永不过期用户等
- **针对管理员的审计**，包括管理员的活动动作、登录、权限、操作等
- **用户可以自定义审计**

实时告警

- **提供实时告警：** SQL注入告警、拖库攻击告警、漏洞利用告警等
- **TOP活动提醒：** 高活跃用户、高活跃IP、高活跃用户角色和高活跃应用等

示例：数据库审计定义和效果呈现

- 客户有个关键的用户信息表，希望审计所有对该表的查询以及操作。
- 使用数据库审计功能，先创建审计的规则（已经提前配置好了远端数据库）

示例：数据库审计定义和效果呈现

- 所有对数据库的查询都已经记录

FusionGuard HexaTier：报告

报告标题: 操作日志

报告日期: 2018-05-03 17:39:37

编号	ID	审计日期	查询概要	数据库	用户名	客户端IP
1	4	2018-05-03 17:38:32	UPDATE TABLE `confidential`.`userinfo`	confidential	root	客户端操作的IP
2	3	2018-05-03 17:38:05	SELECT FROM TABLE `confidential`.``.`userinfo`	confidential	root	客户端操作的IP
3	2	2018-05-03 17:38:01	SELECT FROM TABLE `confidential`.``.`userinfo`	confidential	root	客户端操作的IP
4	1	2018-05-03 17:37:48	SELECT FROM TABLE `confidential`.``.`userinfo`	confidential	root	客户端操作的IP

总结：三步打造云上数据库安全

Before 事前

Detection 事中

After 事后

数据泄露保护 DLP

- 敏感数据发现
- 动态数据脱敏

数据库防火墙 DBF

- SQL注入防御
- 责权分离
- 漏洞检测防御
- 合规检查
- 拖库检测

数据库审计防护 DAP

- 数据库活动监控
- 合规报表
- 日志分析

总结：关于数据库安全部署时的几点建议

- 如果数据库正在“裸奔”，先到漏洞库公告网站（如CNNVD，CNCERT或数据库官网等）查询并打上补丁，并立即制定安全防护方案
- 对您的数据库中类型、数据保密等级进行分析，高价值资产优先保护
- 考虑数据库安全部署方式的时候，统筹考虑审计、脱敏、防火墙等功能
- 法律法规的要求需要立即遵从，不要等罚款时再整改
- 培养DBA和数据库运维人员的信息安全和风险管理意识，安全永远不但是技术问题，还是管理问题

THANK YOU