Tencent 腾讯 | 腾讯云

守卫安全 创造价值

——公有云平台的风险感知能力建设实践——

周斌

2015.11

关于我

- 2005年加入腾讯
- 负责支付和安全系统的建设工作
- 目前专注腾讯云安全工作
- 关注技术点：海量数据处理、高性能server、安全技术

- 微信：bblue9

腾讯云-打造一站式云端生态

腾讯云是全球领先的公有云服务提供商，主要定位服务于广阔的企业级用户市场。基于QQ、微信、QQ空间、腾讯游戏等海量业务的技术架构和精细化互联网运营经验，腾讯云不仅能提供普适的云计算基础设施服务，还提供市场稀缺的移动互联网业务的云服务，以及物联网时代的云服务。

Tencent 腾讯 | 腾讯云

目录

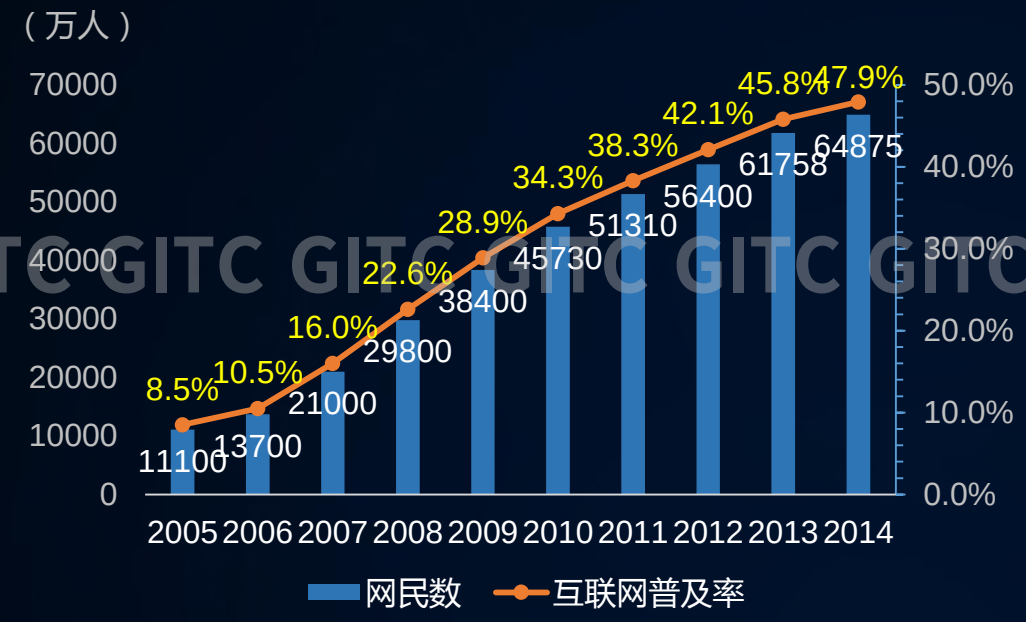
Tencent 腾讯 | 腾讯云

当下是一个怎样的时代？

Tencent 腾讯 | 腾讯云

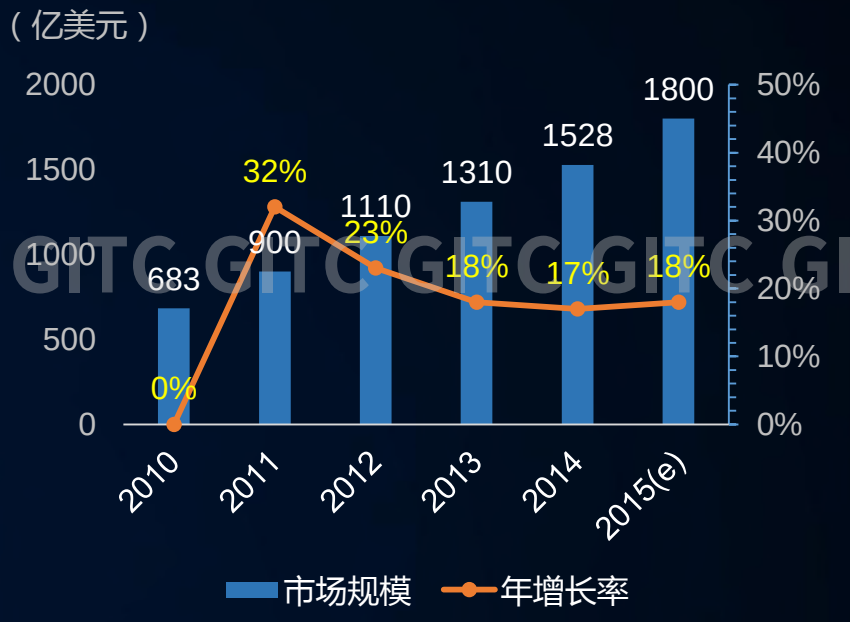
这是最好的时代

这是信息引领社会前进的时代，这是互联网+的时代



中国网民规模和互联网普及率

来源：CNNIC 2014.12



2010-2015年全球云计算市场规模示意图

来源：Gartner 2015.2

Tencent 腾讯 | 腾讯云

服务器规模不断扩大

x 百万

Tencent 腾讯 | 腾讯云

风险很多

稳定性　　数据安全

性能

网络安全

硬件问题

体验问题

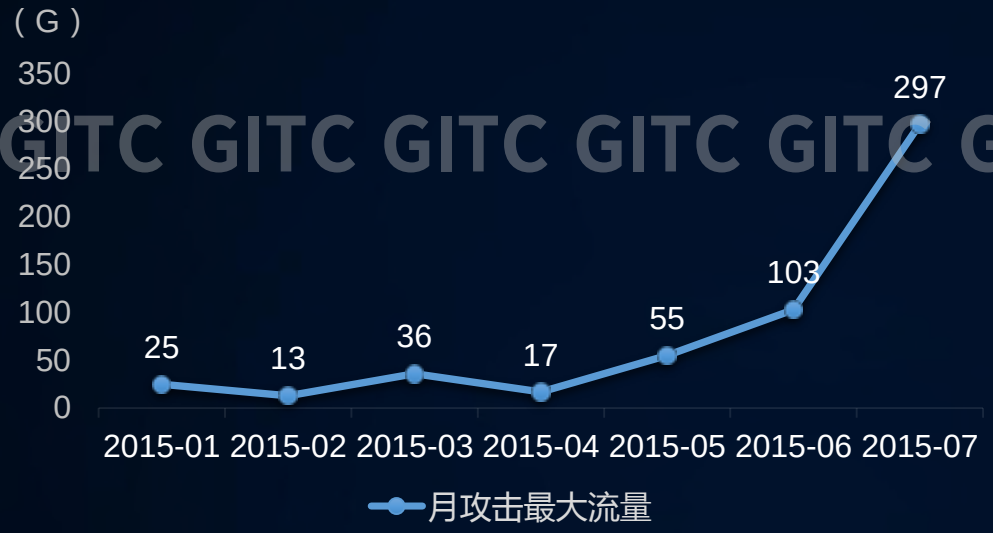
运维性　　稳定性　　…

这也是个糟糕的时代

DDoS肆虐、黑产横行，阻碍互联网的发展

2014.12，国外某知名厂商遭DDoS攻击，服务中断12小时

2015H1国内发生流量超过100G的DDoS攻击33起，国内某厂商遭DDoS攻击，客户业务中断2小时



腾讯云大禹2015H1DDoS防护示意图

- 虚假订单占据**40%**
- 刷单人员超过20万
- 职业刷单人可月入10万

O2O打车行业刷单严重

数据来源：《2015腾讯云安全白皮书》

Tencent 腾讯 | 腾讯云

风险无处不在

icloud被无限次验密爆破

Gmail被撞库，550w账户密码泄漏

Sony PSN被入侵，7700w用户信息泄漏

More...

Tencent 腾讯 | 腾讯云

一边是海水一边是火焰

公有云需要一个怎样的安全风险感知系统？

体验

精准

性能

隐私

覆盖

Tencent 腾讯 | 腾讯云

从公有云基础架构开始

腾讯云的基础架构

静态加速用图片等内容，动态加速智能选路，优化传输路径

TGW外网统一接入集群，外网IP和虚拟机解耦，四七层负载均衡，防御各种DDOS攻击

内网负载均衡，访问后端存储服务和自己搭建的服务

租户之间网络隔离，双向流量限制

VM之间带宽基于HTB的QoS控制

存储网络和业务网络分离，互为备份

Tencent 腾讯 | 腾讯云

愿景

监控系统？No，我们的目标是感知安全风险

目标：

- 异常发现
- 数据联动分析
- 拦截
- 覆盖
- 准确

重点：成本（体验）与安全性的平衡

思路

Tencent 腾讯 | 腾讯云

关于预测

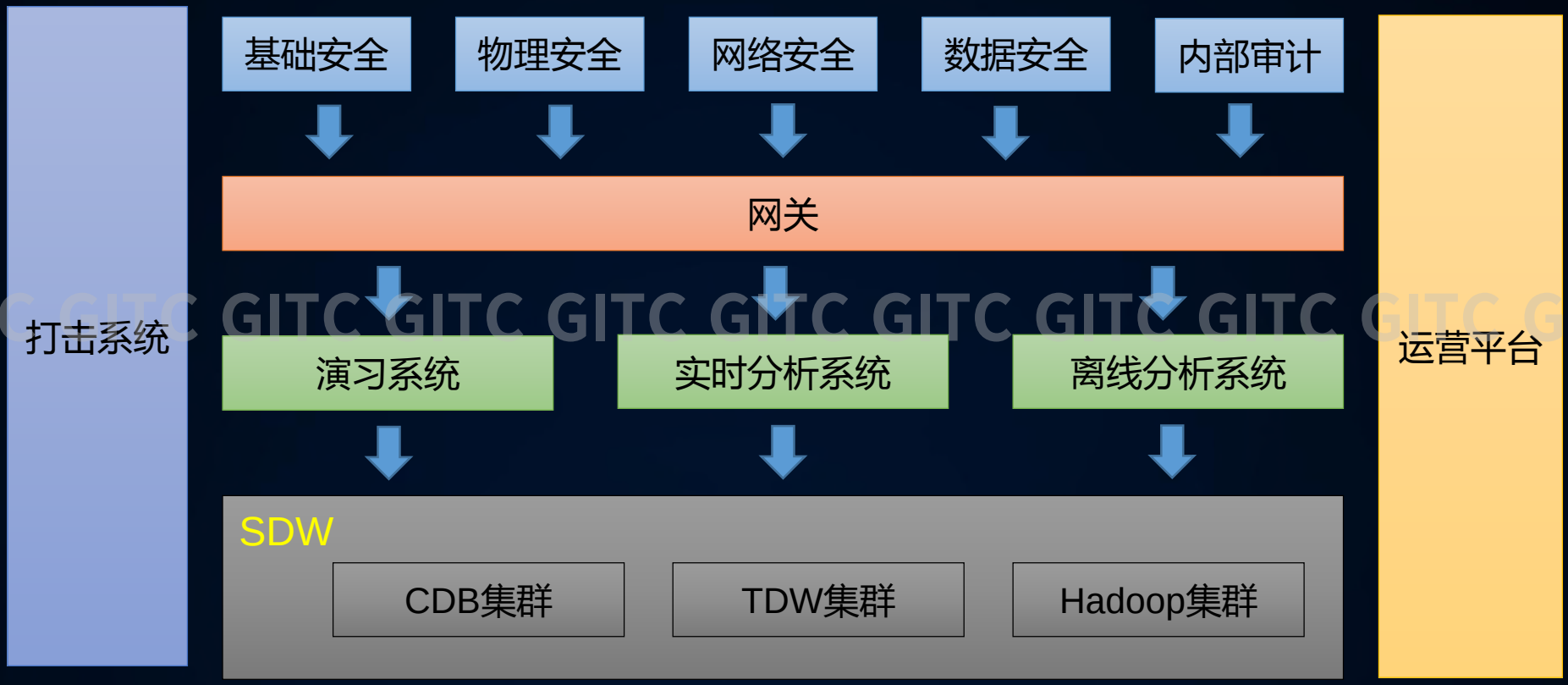
为什么要预测？

为什么不要预测？

基于海量的数据计算，细微处可见真章

Tencent 腾讯 | 腾讯云

腾讯云安全感知架构



数据规模：3P 数据，每日计算量：6609亿

Tencent 腾讯 | 腾讯云

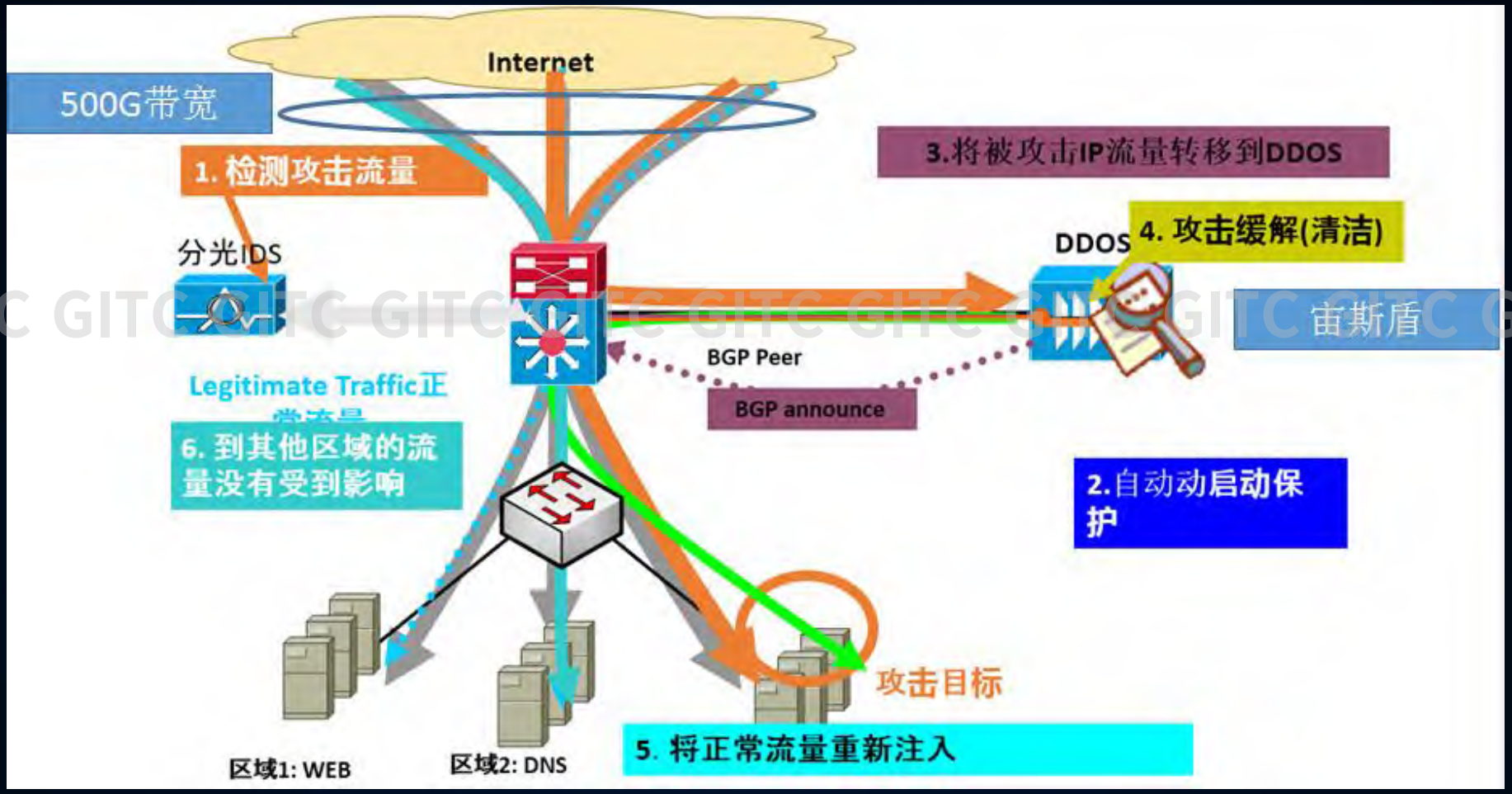
基础平台安全

隔离

- 基于虚拟化的隔离（Xen、Kvm）
- 网络层隔离
- 基础组件与用户隔离
- IDC间隔离

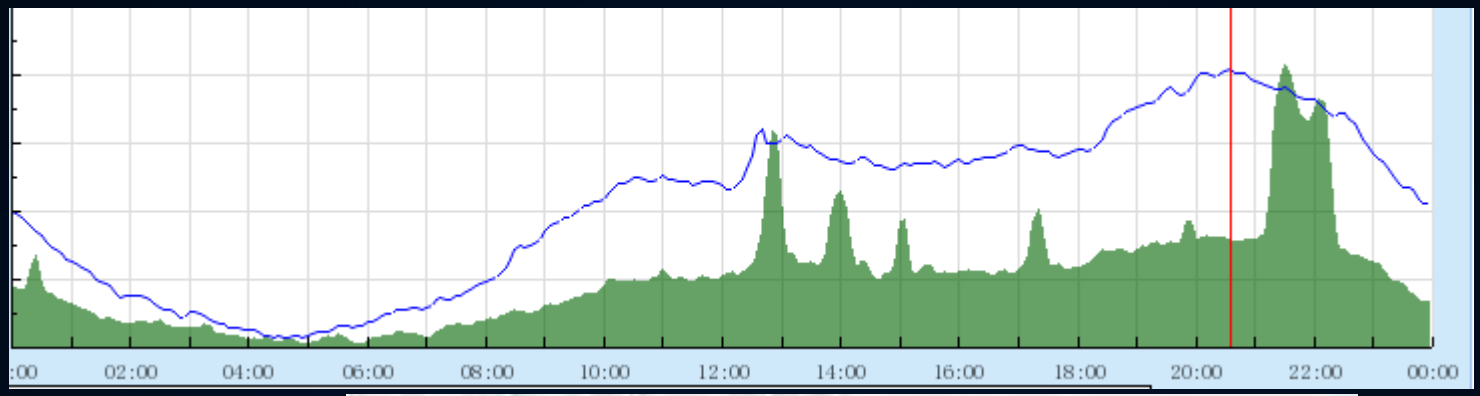
Tencent 腾讯 | 腾讯云

网络安全—宙斯盾

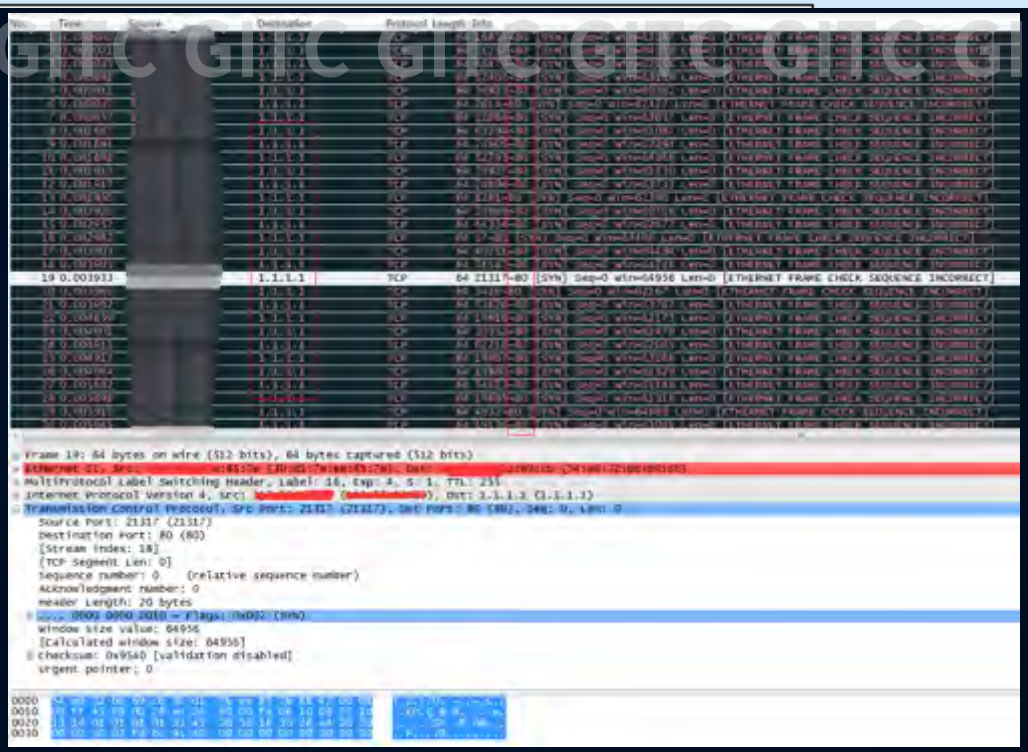


流量分析模型

某个IDC出口流量图



异常流量



Tencent 腾讯 | 腾讯云

三度问题

模块安全功能

Tencent 腾讯 | 腾讯云

分类

云中的四个角色

风险分类	范围
数据安全	资料安全
	通信安全
	安全合规
平台安全	支撑软件
	安全产品
	连续性管理
	物理安全
流程规范	权限管理
	研发规范
内部审计	审计

三个永恒的话题：权限、加密、检测

权限

- 如何进行权限控制？
- 端到端的四把钥匙验证
  - 1.用户票据（证明是用户A）
  - 2.用户数据权限（证明A有拉此数据的权限）
  - 3.业务签名（证明是业务B）
  - 4.业务数据权限（证明B有拉此数据的权限）

- 为什么要验证业务？
  - 业务场景合规才能给权限
  - 黑客入侵、内鬼

加密

- 案例
  - 600w、4000w、93
  - 一次MD5 1亿+
- 密钥管理
  - 密钥长度（如RSA1024bit以上、TEA32轮等）
  - 密钥更换（怎么换？）
  - 密码一次MD5，拼密钥
- 关于密码破解
  - 暴力
  - 弱密码
  - 字典
  - 彩虹表
  - 怎么应对？

aaaaaa -H()->281DAF40 -R()-> sgfnyd -H()-> 9203CF10 --R()-->kibgt.

检测

水印 + 蜜罐 + 策略

- 定性到定量
- **微软的“DREAD”评分标准**
  - 潜在破坏性
  - 可再现性
  - 可利用性
  - 受影响的用户
  - 可发现性
- **我们的“ALSOM”（Awesome）评分标准**
  - 协议级别 Affected data 影响数据种类 2
  - 可能泄漏量 Leak magnitude 影响数据量级 1
  - 业务类型 Service type 宏观业务类型 3
  - 可能动机 Motivation 个体行为动机 2
  - 其他维度 Other 其他可疑信息 2

一个成熟的安全体系，对异常事件的威胁度，应可给出定量分析

平台安全

基线扫描

基线类型	基线数
网络访问控制	11
通用软件基线	10
系统鉴权	21
数据加密	8
DDoS攻击防范	19
业务可靠和连续性	6
入侵检测与防范	10
操作审计	11
漏洞扫描与修复	6
软件开发安全	10
操作安全	8
物理安全	1
人力资源安全	2
安全组织	1
安全策略	1

人工流程

NOC
安全团队

物理区域控制

流程规范

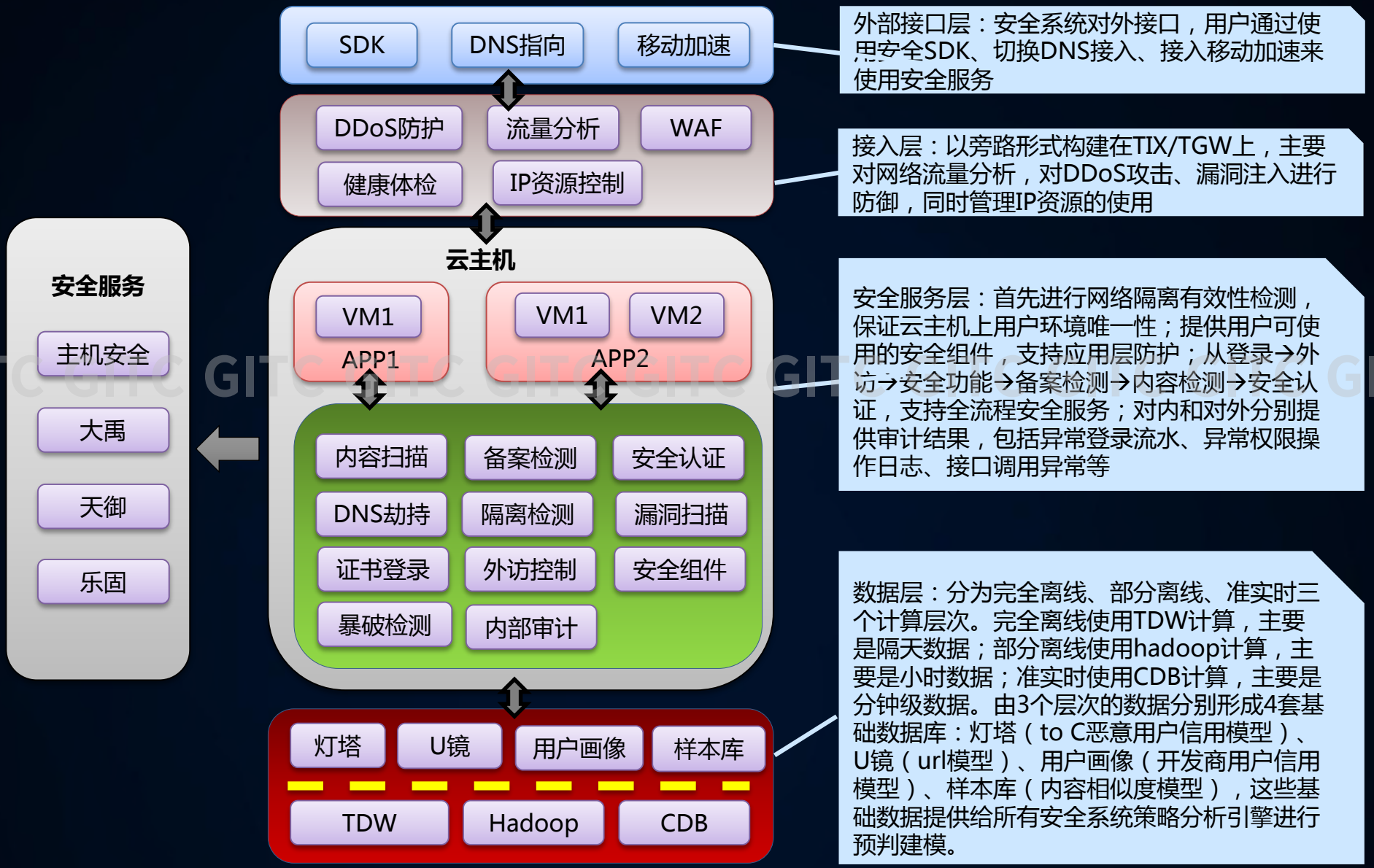
权限、Log、web化、实时

构建信任边界

安全的本质是信任

- 完善的安全功能
  - ✓数据齐全
  - ✓检测、防护、分析
- 严密的鉴权机制
  - ✓ 确认每个环节集中鉴权
- 可靠的审计结果
  - ✓ 代码审计
  - ✓ Double check
  - ✓ 操作审计

安全体系架构



外部接口层：安全系统对外接口，用户通过使用安全SDK、切换DNS接入、接入移动加速来使用安全服务

接入层：以旁路形式构建在TIX/TGW上，主要对网络流量分析，对DDoS攻击、漏洞注入进行防御，同时管理IP资源的使用

安全服务层：首先进行网络隔离有效性检测，保证云主机上用户环境唯一性；提供用户可使用的安全组件，支持应用层防护；从登录→外访→安全功能→备案检测→内容检测→安全认证，支持全流程安全服务；对内和对外分别提供审计结果，包括异常登录流水、异常权限操作日志、接口调用异常等

数据层：分为完全离线、部分离线、准实时三个计算层次。完全离线使用TDW计算，主要是隔天数据；部分离线使用hadoop计算，主要是小时数据；准实时使用CDB计算，主要是分钟级数据。由3个层次的数据分别形成4套基础数据库：灯塔（to C恶意用户信用模型）、U镜（url模型）、用户画像（开发商用户信用模型）、样本库（内容相似度模型），这些基础数据提供给所有安全系统策略分析引擎进行预判建模。

Tencent 腾讯 | 腾讯云

安全服务

基础服务

- DDoS防护
- WAF
- 云主机防护

高级服务

- DDoS高防
- 大禹（网站安全防护）
- 天御（业务安全防护）
- 乐固（移动安全防护）
- 专家服务

云内安全未来趋势

大数据时代的挑战，安全问题最终还是数据问题

- 海量数据与性能的权衡
- 安全边界模糊，手法更多样
- 权限管理与灵活体验平衡
- 新技术对安全体系穿透

Tencent 腾讯 | 腾讯云

腾讯云安全白皮书

欢迎下载查看


Q&A
Thanks!
GITC GITC GITC GITC GITC GITC GITC GITC GITC GITC GITC GI