混合云态势感知安全解决方案

主讲人：戈建勇

议题

1. 混合云发展趋势及面临的挑战。

2. 混合云态势感知安全解决方案。

3. 几种不同场景下的态势感知安全解决方案。

混合云成为企业过渡方案的必然选择

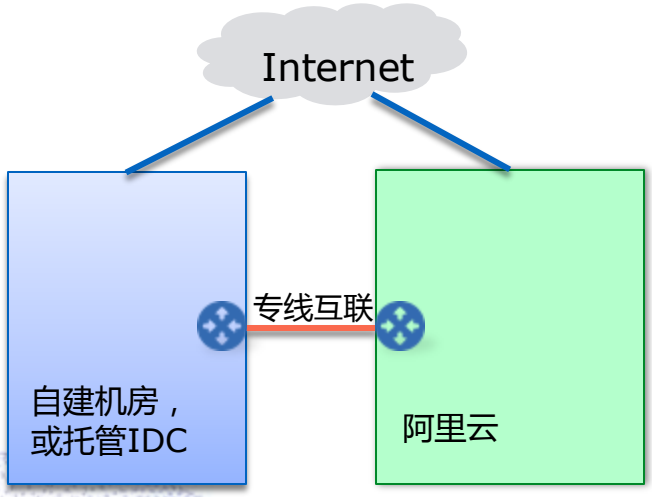
公共云

另一方面，公共云技术快速发展，企业为了享受云计算的便利性，降低整体IT投资，越来越拥抱云的变革。

传统数据中心

一方面，由于种种原因，客户依然将长期保留在传统数据中心的固有投资。

混合云场景对安全上的挑战

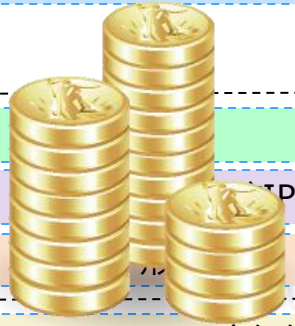


挑战

- 对传统IDC的安全体系比较熟悉，云上业务如何保证安全？
- 云上安全比云下有何差异？
- 如何统一管理云上和云下的安全系统？
- 云下安全的投入上百万，每隔3-5年又要更新换代，是否有节省安全投资的办法？

传统安全体系到云安全体系的转变

	传统数据中心	阿里云
	渗透测试服务	先知计划
事后 - 安全事件管理	S	
事中 - 网络入侵检测	硬件	态势感知
事前 - 漏洞检测		
主机层攻击防护		
网络层DDoS攻击防护		
Web应用层攻击防护		
网络隔离和访问控制	硬件防火墙	VPC - 租户级的隔离 第3方安全镜像 - 租户南北向访问控制 安全组 - 租户东西向访问控制



传统安全架构

- 盒子化交付，周期长
- 难以弹性扩展
- 离线
- 情报少
- 规则+正则

云安全架构

- 敏捷：SaaS化交付，分钟级
- 弹性：按需、随时弹性扩展
- 在线：规则实时更新
- 数据情报：漏洞、威胁、事件、人员
- 计算及模型能力：增强未知威胁检测能力

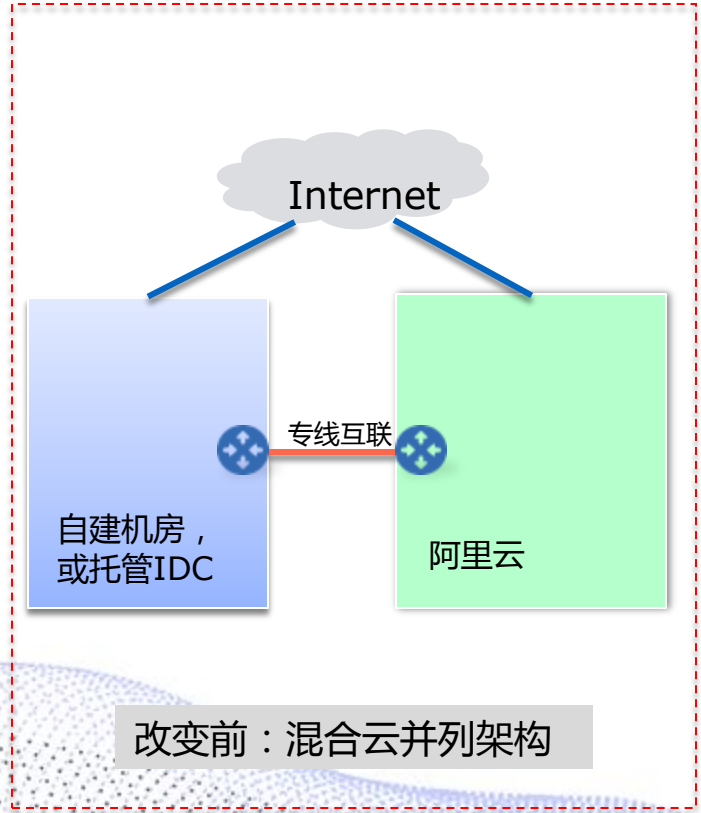
难道需要在混合云环境，重复建设两套不同的安全体系？

议题

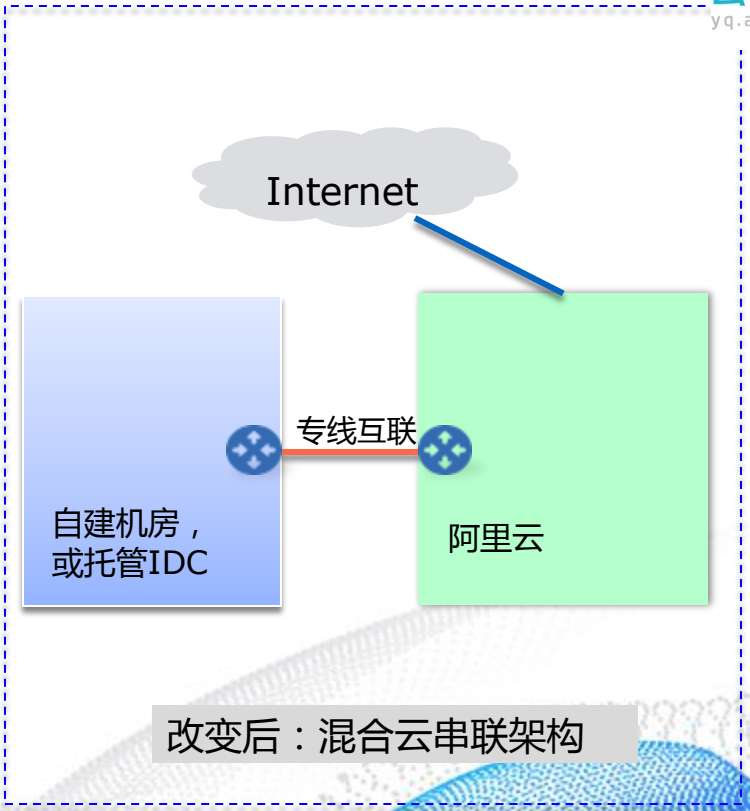
1. 混合云发展趋势及面临的挑战。

2. 混合云态势感知安全解决方案。

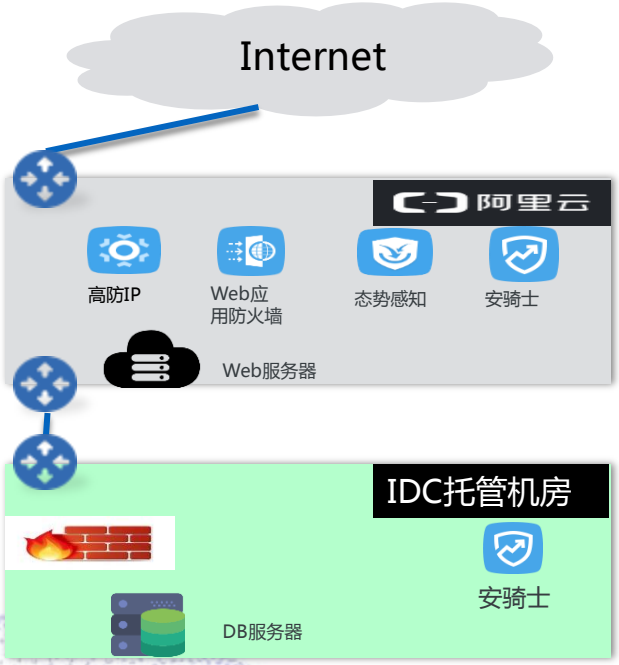
3. 几种不同场景下的态势感知安全解决方案。



改变前：混合云并列架构



改变后：混合云串联架构



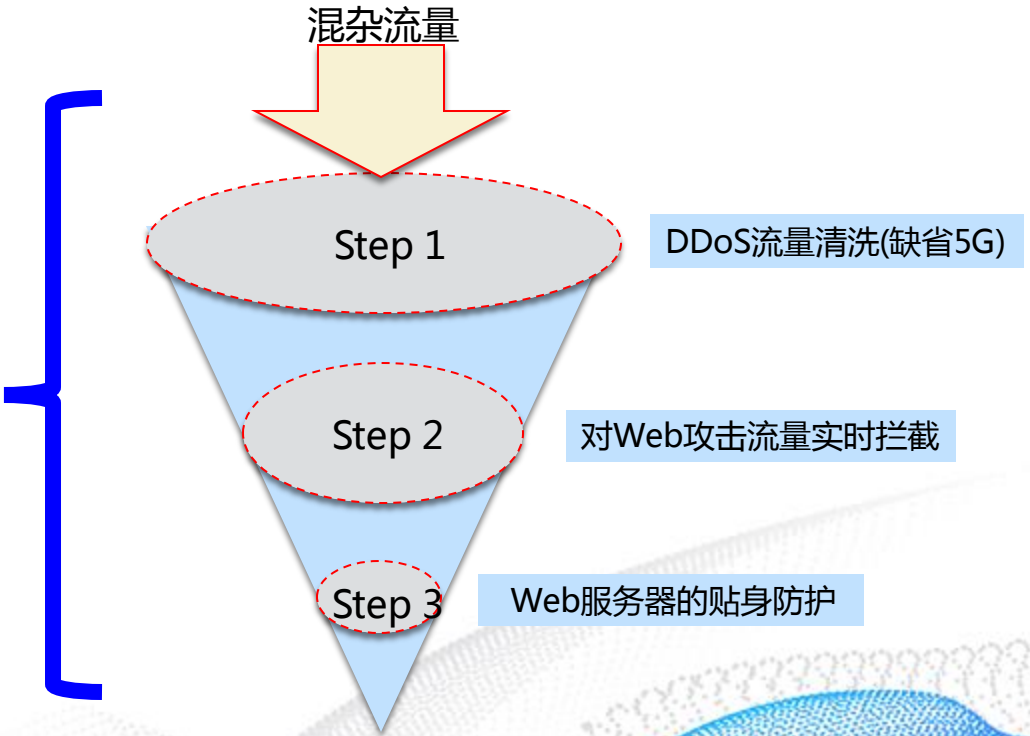
解决方案

- Step1，将互联网出口应用全部署在阿里云，数据库等核心数据任然部署在线下机房，所有互联网的访问都必须经过阿里云。
- Step2，在IDC托管机房，只需要配置硬件防火墙用于安全域的隔离。
- Step3，在阿里云开启DDoS高防、WAF、安骑士等安全防护能力。
- Step4，通过在IDC的服务器上部署安骑士agent，通过云盾.态势感知实现混合云安全的统一管理。

客户价值

- 统一管理混合云安全策略。
- 减少运维成本和对线下安全硬件的投入。
- 安全、弹性、便捷的阿里云层。

基于大数据和威胁情报的态势感知， 实时监控防御效果。



第一重防护：基于web流量的实时过滤

Web防护

- ✓ 防数据泄露、避免网站挂马
- ✓ 防御恶意DDoS和CC攻击
- ✓ 地理区域IP封禁

网页防篡改

- ✓ 对指定的敏感页面进行缓存

业务风控

- ✓ 防垃圾注册、刷库撞库
- ✓ 防活动作弊、论坛灌水
- ✓ API接口防刷

第二重防护：服务器的贴身防护

木马查杀

- ✓ 顶级Web shell查杀
- ✓ 云+端的查杀体系
- ✓ 秒级发现后面文件并预警

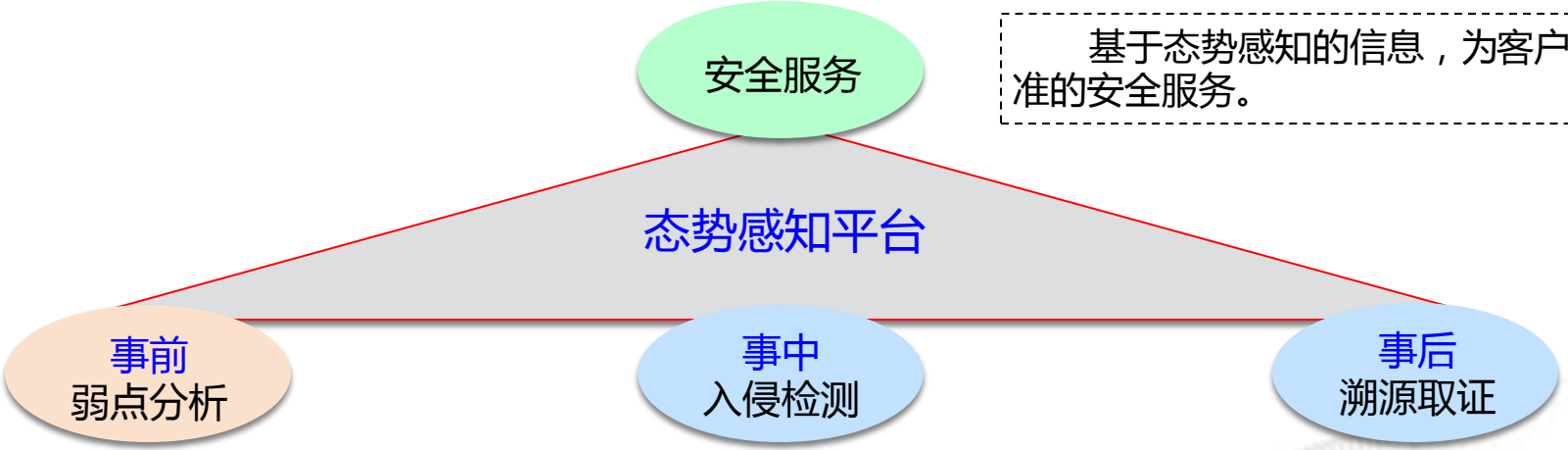
补丁管理

- ✓ 通用web软件漏洞
- ✓ Windows系统漏洞
- ✓ 灰度更新，一键回滚

安全巡检

- ✓ 账户安全监测
- ✓ 弱口令检查
- ✓ 配置风险检测

第三重防护：基于态势感知的安全服务



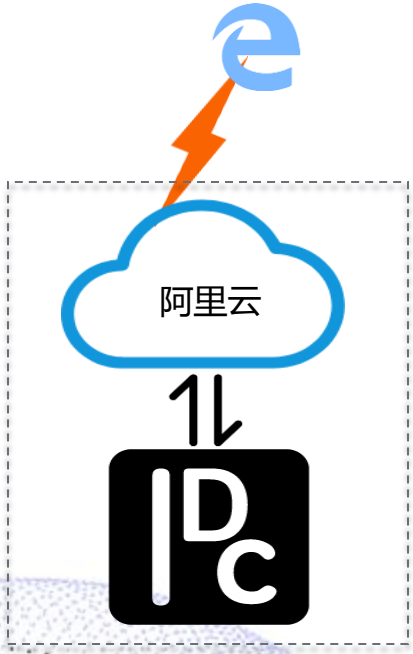
基于态势感知的信息，为客户提供精准的安全服务。

- ✓ Web漏洞、主机漏洞
- ✓ 配置隐患、弱口令检测

- ✓ 页面篡改的监控
- ✓ Web入侵的实时拦截（WAF）

- ✓ 从黑客发起攻击到攻破系统，进行数据盗取的全过程还原。
- ✓ 全量http日志的采集和TB级大数据量的处理

1、业务运营监控　2、安全应急响应中心 3、安全感知体系　4、安全防御体系　5、业务访客分析
6、业务稳定性监控 7、网络层安全态势　8、主机层安全态势 9、主机连接拓扑　10、实时安全态势和安全评分



便捷、弹性

网络、计算、存储、安全系统的快速部署即开即用，弹性扩展。

安全

共享全网威胁情报，阿里云成为一个安全的云接入层。

统一管理

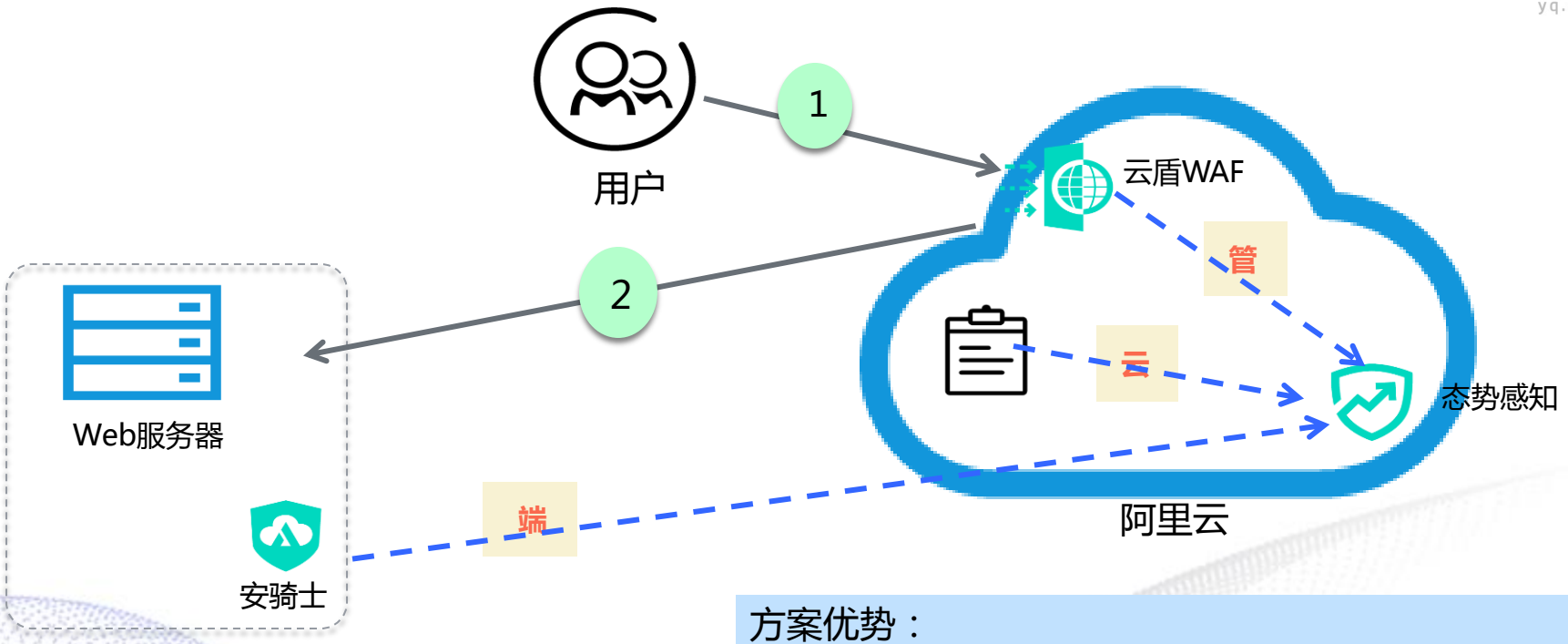
基于大数据的安全态势感知，统一管理混合云安全策略。

议题

1. 混合云发展趋势及面临的挑战。

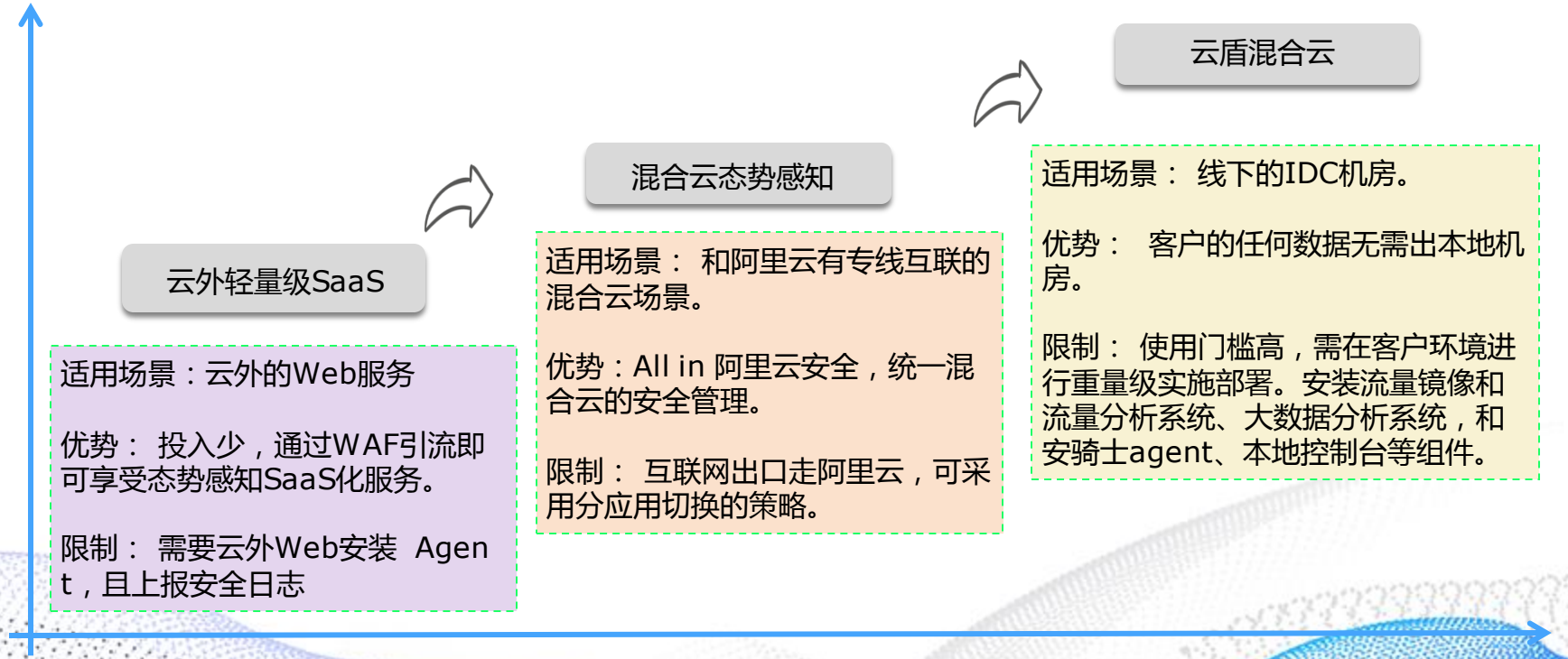
2. 混合云态势感知整体解决方案。

3. 几种不同场景下的态势感知安全解决方案。



方案优势：

1、客户系统无需在阿里云上，即可享受大数据安全的态势感知服务。
2、管道的web全流量实时分析和攻击拦截。
3、共享云上威胁情报，全量大数据的实时分析监控。


云外轻量级SaaS
适用场景：云外的Web服务
优势： 投入少，通过WAF引流即可享受态势感知SaaS化服务。
限制： 需要云外Web安装 Agent，且上报安全日志
混合云态势感知
适用场景： 和阿里云有专线互联的混合云场景。
优势：All in 阿里云安全，统一混合云的安全管理。
限制： 互联网出口走阿里云，可采用分应用切换的策略。
云盾混合云
适用场景： 线下的IDC机房。
优势： 客户的任何数据无需出本地机房。
限制： 使用门槛高，需在客户环境进行重量级实施部署。安装流量镜像和流量分析系统、大数据分析系统，和安骑士agent、本地控制台等组件。

习总书记的安全观

核心事实 2016年4月19日，中共中央总书记、国家主席、中央军委主席、中央网络安全和信息化领导小组组长习近平主持召开网络安全和信息化工作座谈会并发表重要讲话。会议对当前我国互联网建设和发展中遇到相关问题均指出了明确的方向。

习总书记“4•19”重要安全语录：

- 网络安全是整体的而不是割裂的。
- 网络安全是动态的而不是静态的。
- 那种依靠装几个安全设备和安全软件就想永保安全的想法已不合时宜，需要树立动态、综合的防护理念。
- 全天候全方位感知网络安全态势。知己知彼，才能百战不殆。没有意识到风险是最大的风险。网络安全具有很强的隐蔽性，一个技术漏洞、安全风险可能隐藏几年都发现不了，结果是“谁进来了不知道、是敌是友不知道、干了什么不知道”，长期“潜伏”在里面，一旦有事就发作了。
- 维护网络安全，首先要知道风险在哪里，是什么样的风险，什么时候发生风险，正所谓“聪者听于无声，明者见于未形”。感知网络安全态势是最基本最基础的工作。要全面加强网络安全检查，摸清家底，认清风险，找出漏洞，通报结果，督促整改。要建立统一高效的网络安全风险报告机制、情报共享机制、研判处置机制，准确把握网络安全风险发生的规律、动向、趋势。

全文：http://news.xinhuanet.com/politics/2016-04/25/c_1118731175.htm


2017云栖大会·成都峰会
THE COMPUTING CONFERENCE
阿里云
云栖社区
yq.aliyun.com
飞天·智能
APSARA INTELLIGENCE
2017云栖大会·成都峰会
5月23日 成都世纪城天堂洲际大酒店