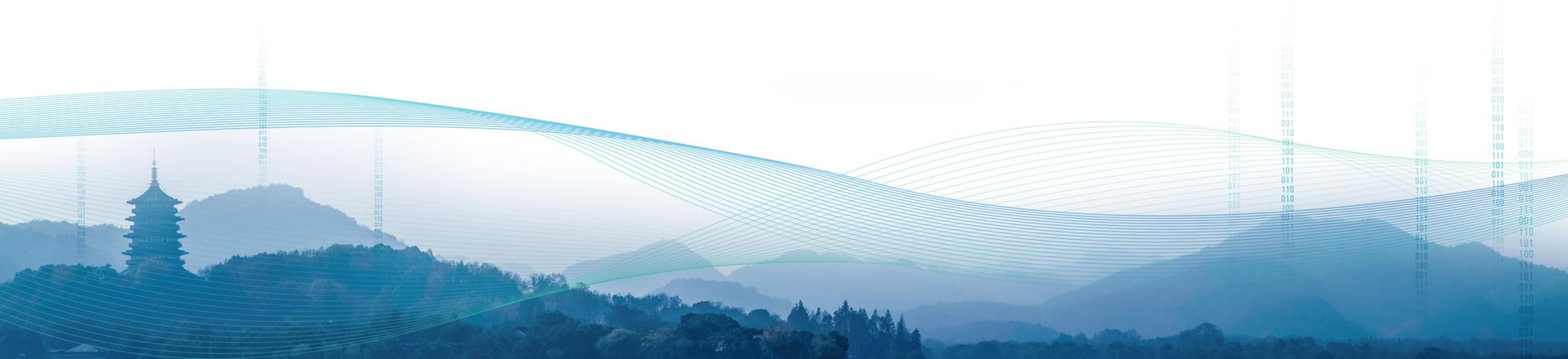
2019 西湖论剑·网络安全大会
WEST LAKE CYBERSECURITY CONFERENCE

《运营商云安全解决方案新思路》

主讲人：贾腾飞

PART 01 统一监控与防护平台在集约化背景下的应用:降本



现实背景

自营业务系统分散

有托管在运营商自己的云上的
有部署在地市各个机房的

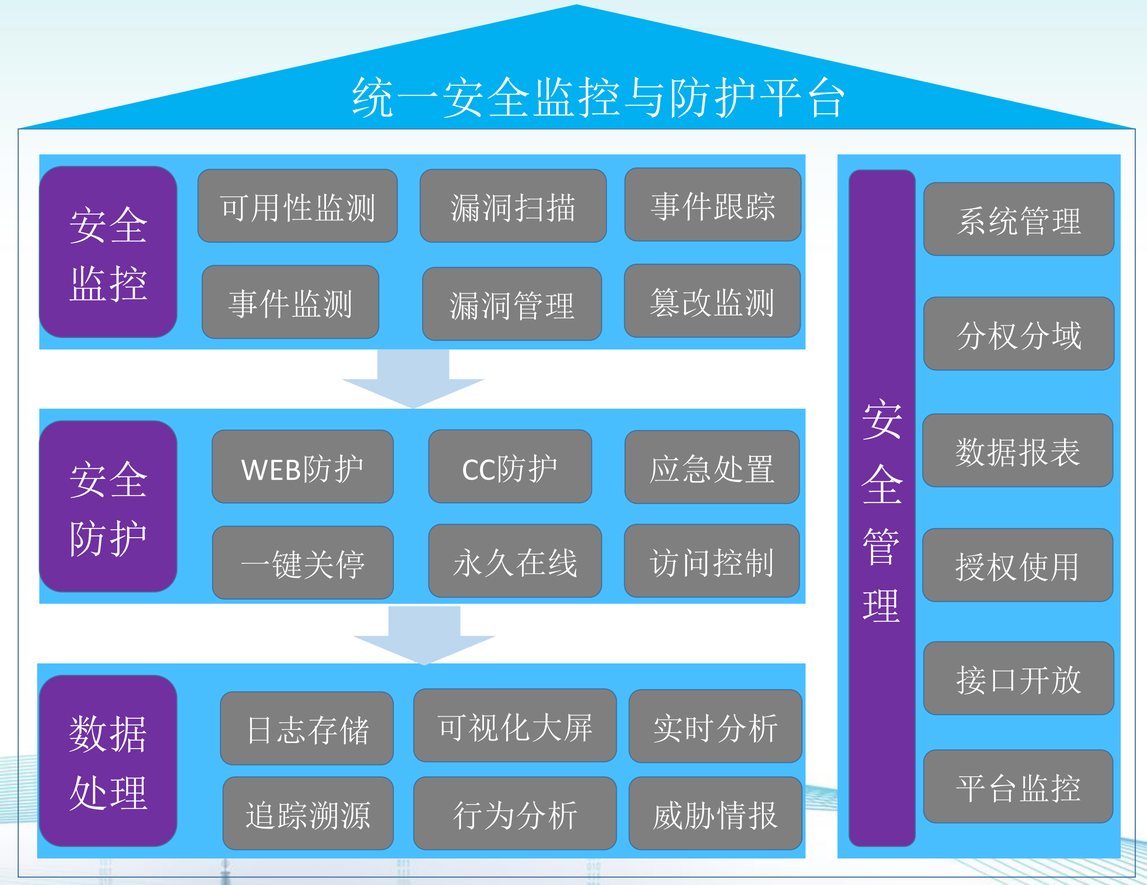
缺乏统一运维管理

有IP访问的，有域名访问的
防护能力参差不齐

两部委和集团考核

面临考核前临时抱佛脚
紧急做安全评估和加固

统一安全监控与防护平台方案思路



安全监测：监测系统安全风险和安全事件，且支持第三方风险数据导入

事件审核：针对安全风险进行告警审核，数据标签化

督促整改：通过平台配置责任人，邮件短信进行整改通知下发

复验闭环：修复后通过平台提交整改结果，验证通过后关闭事件，形成闭环

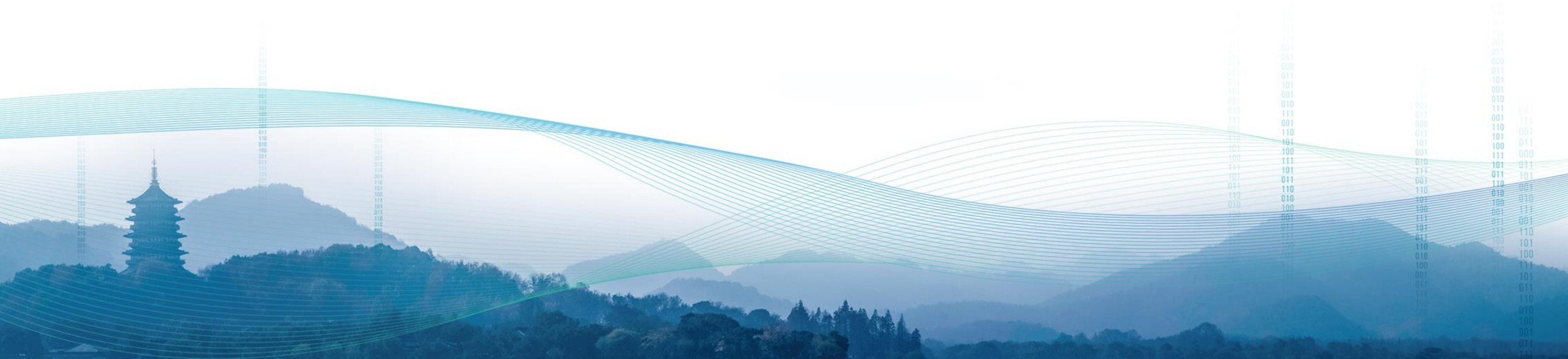
统一防护：机器学习+防护规则双重防护，防入侵，防篡改，防泄露

应急处置：防护失效时，通过平台可分钟级关停网站或者恢复网站正常页面

统一管理：账号分级管理，落实安全责任制度，找到人，找对人

方案意义

PART 02 统一监控与防护平台在云化背景下的应用:增效

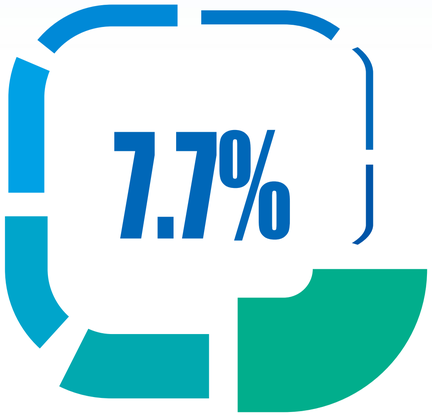


上云趋势愈演愈烈

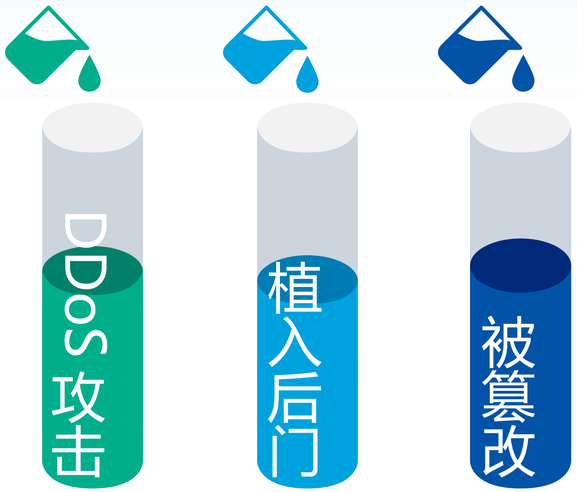
工信部〔2018〕135号印发了《推动企业上云实施指南(2018-2020年)》的通知

百万企业上云的背景下，运营商成为获益方，如何针对这部分上云的业务实现安全增值服务是运营商的一大机遇也是挑战。

云计算场景下安全背景



主流云平台使用IP占比



云平台网络攻击占比

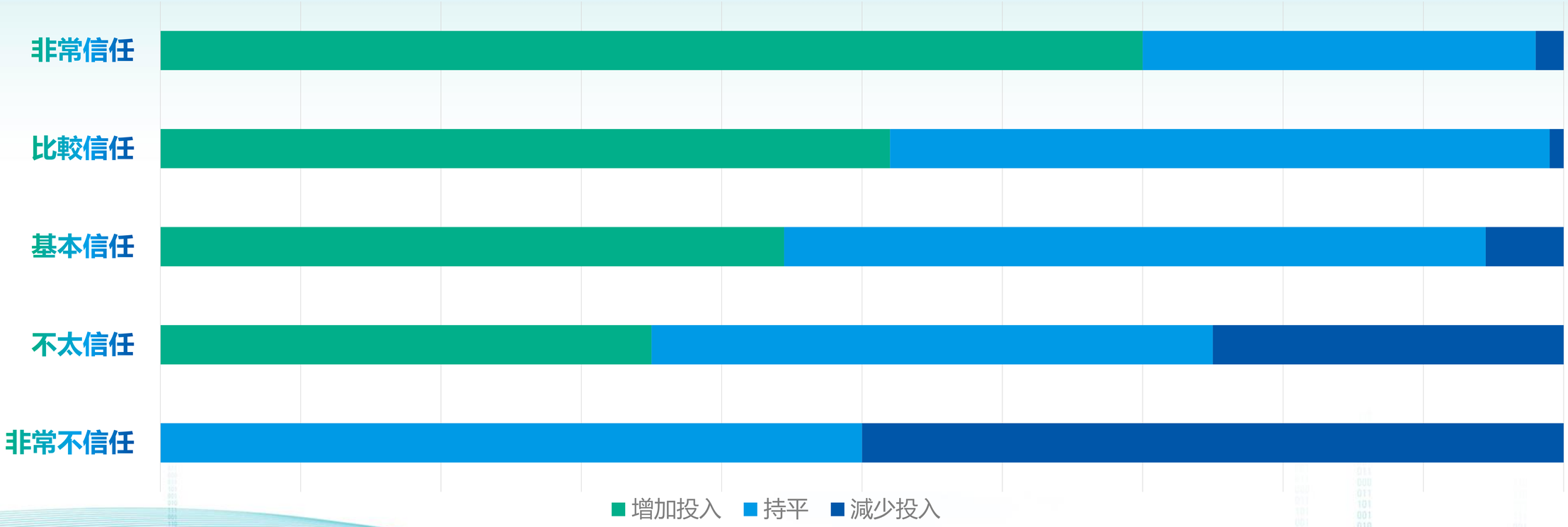
现状：云平台已成为发生网络攻击的重灾区

原因：云服务存在便捷性、可靠性、低成本、高带宽、高性能和复杂性等特性

问题：云平台用户认为上云了安全就得云厂商负责

结论：云服务商和云用户都应加大对网络安全的重视和投入

越安全，越可信



报告也发现，对云的信任度越高，越愿意在企业安全上投入

Web安全、DDoS防御、主机安全仍然是企业在安全上投入的“三大件”

安全服务解决方案

01

事前体检

- 安全体检
- 事件验证
- 通知下发
- 复验关闭

02

事中防护

- DDoS清洗
- WEB防护
- 一键关停

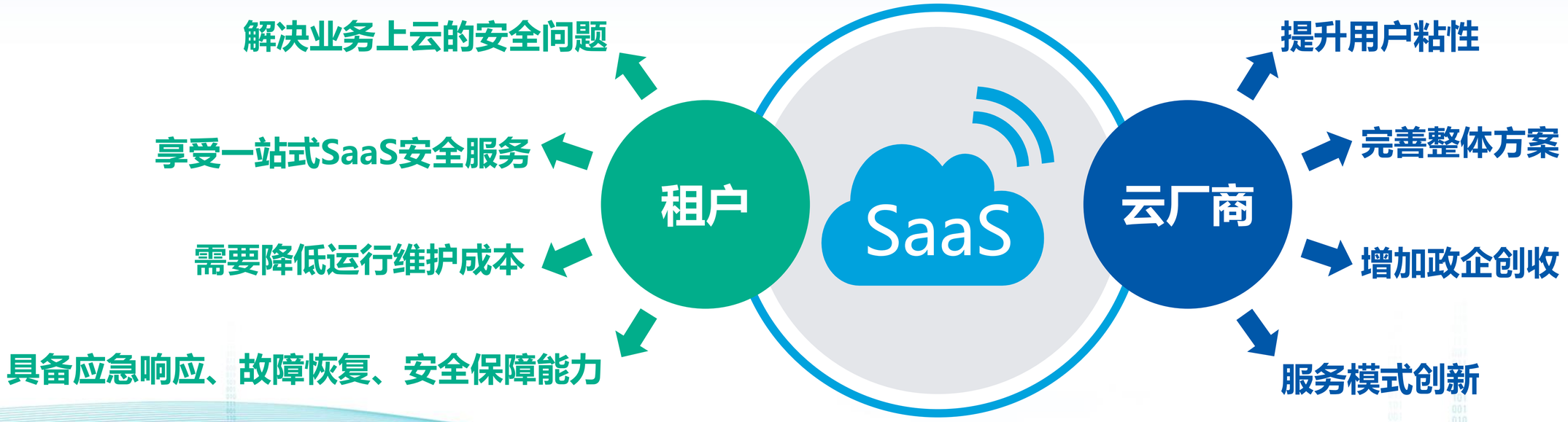
03

事后分析

- 数据分析
- 追踪溯源
- 安全展示
- 7*24服务

云服务商引入可信的第三方安全厂家，提供一站式网站与应用系统SaaS云安全解决方案

服务创造价值


解决业务上云的安全问题
享受一站式SaaS安全服务
需要降低运行维护成本
具备应急响应、故障恢复、安全保障能力
租户
SaaS
云厂商
提升用户粘性
完善整体方案
增加政企创收
服务模式创新

THANK YOU

谢　　谢　　观　　看