



2016 杭州·云栖大会
THE COMPUTING CONFERENCE

云栖社区
yq.aliyun.com

让租户 安全快速上云 让云服务商 业务增值

——构建开放、跨云的云安全平台

深信服 殷浩 安全BU CTO

2016
The Computing Conference

主办单位：



Alibaba Group
阿里巴巴集团

战略合作伙伴：



扫码观看大会视频

云：从混沌到清晰

技术

标准

政策

虚拟化



超融合



云计算

缺乏标准



云等保标准



政务云标准

国务院



工信部



省级政府



政务云：正在加速前行

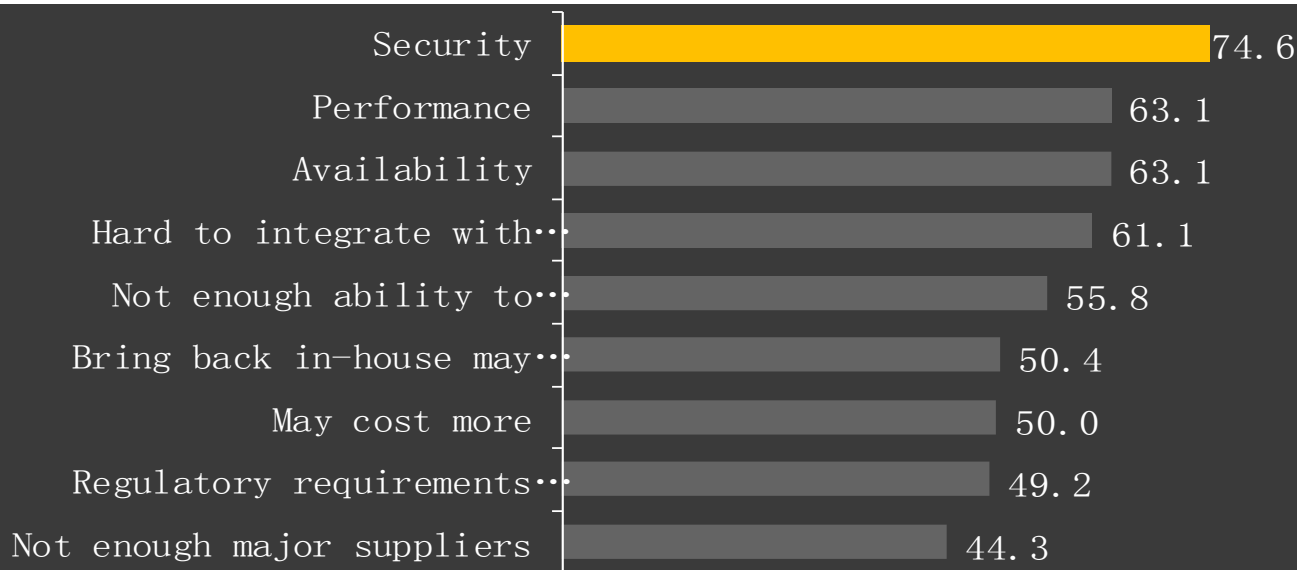
附件：省直部门应用系统 2016 年迁移计划表

	省直部门	应用系统名称	部署网络	类型	是否涉密	完成时间
1	省发改委	内部综合办公系统	专网	内部政务服务类	否	2016 年 10 月
2		内部业务审批系统	专网	专业应用类	否	2016 年 11 月
3		内部电子监察系统	专网	专业应用类	否	2016 年 11 月
4		门户网站	互联网	互联网政务服务类	否	2016 年 10 月
5		外网政务服务平台	互联网	专业应用类	否	2016 年 10 月
6		移动办公平台	专网	内部政务服务类	否	2016 年 10 月
7		投资项目管理信息系统	互联网	专业应用类	否	2016 年 11 月
8		联合审批平台	互联网	专业应用类	否	2016 年 11 月
9		宏观经济大数据平台	互联网	专业应用类	否	2016 年 10 月



云计算所面临的挑战中，安全问题排在首位

75%用户在安全性上犹豫不决



Source: IDC Enterprise Panel (国际数据公司IDC)



扫码观看大会视频

政务云安全两大问题

一：巧妇难为无米之炊？

二：只有盾牌就够了吗？





政务云安全责任常见误区

正确的云安全责任认知：
云服务方、租户安全责任共担
系统谁运行，谁负责



政务云租户缺乏完整合规的安全手段

01

阿里云、AWS等云平台
不断完善的安全生态市场



深信服等安全厂商积极参与，
不断推出V系列云端安全方案

02

商业版的政务云
缺乏完善的安全生态



运营商等PPP模式的政务云
聚焦计算、存储、网络基础服务
和平台安全，**缺乏面向租户的安全**



政府租户上云，安全责权不对等

云计算安全服务指南

GB/T 31167

责任：谁运行谁负责

GB/T 2239

云计算等保标准

租户压力

安全尚未资源化、服务化

权利：缺乏安全合规手段

手段单一，防御为主



安全事故板子还是要打在租户身上
租户上云 慢!慢!慢!

急需一套像计算资源按需交付的
安全资源服务



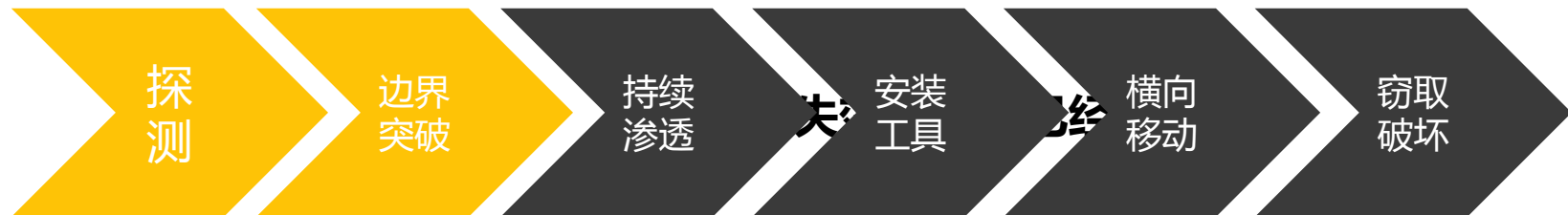
政务云安全两大问题

一：巧妇难为无米之炊？

二：只有盾牌就够了吗？



只有盾牌就足够了吗？



探测
端口扫描
漏洞扫描

Web攻击
应用漏洞攻击
系统漏洞利用
**APT、0day
社工**

提权
获取权限
修改脚本

Web shell
恶意软件
僵尸木马
后门

破解Hash
RDP
漏洞利用
远程控制
跳板攻击

多跳攻击
数据泄露
数据销毁
清除痕迹

70%的投资在：
FW/IPS/AV等防御设备

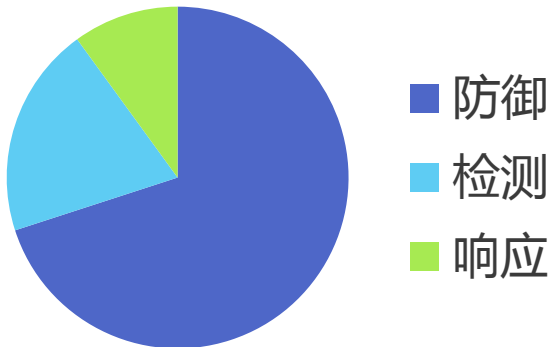
缺乏持续检测的投入



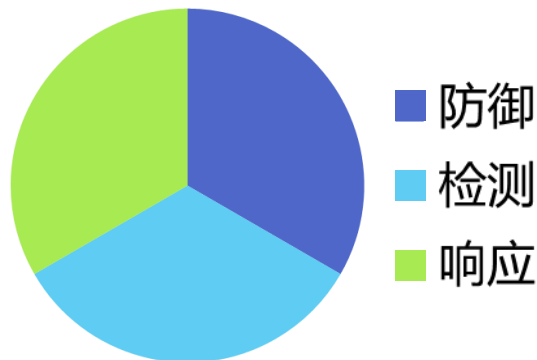
扫码观看大会视频

加大持续检测和快速响应的投入

过去的的安全投资



安全投资的变化



source : Gartner 2014

用户应该大幅提升安全检测手段的投资，应该占到整体安全投资的**30%以上**。
预计到2020年，安全检测和响应的投资将从**10%增长到60%**



扫码观看大会视频

除了防御、检测、响应，还需要什么

GB/T 22239

谁主管谁负责
谁运行谁负责



GB/T 31167

安全管理责任不变
资产的所有权不变
司法管辖关系不变
安全管理水平不变



业务系统安全合规建设

虚拟网络安全

虚拟主机安全

应用系统安全

业务数据安全



合规审计



政务云安全问题带来的风险

运营方

投资难以转换为利润



租户方

业务难以快速上云



监管方

监管职责难以落地







怎么办？




政务云运营建设方的安全需求



安全合规
服务化交付



平台解耦
快速上线



开放合作
生态运营

持续增值和生态运营的政务云 安全资源池



扫码观看大会视频

安全资源池: 平滑扩展、服务化交付、合作共赢

安全合规手段服务化交付

高级防
御服务

失控主机
发现服务

高级防
御服务

数据库审
计服务

运维审
计服务

基础防御
服务

安全接入
服务

失控主机
发现服务

威胁情
报服务

.....

深信服超融合平台



X86服务器

第三方安全服务

深信服安全服务

安全实力

虚拟化实力

云安全资源池方案



扫码观看大会视频

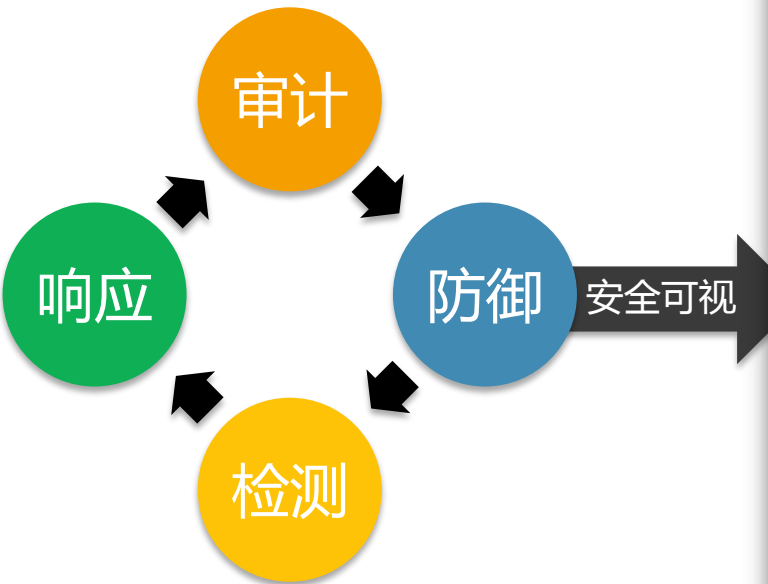
政务云安全资源池方案



深信服云安全资源池



既合规，又有效的安全服务目录



扫码观看大会视频

安全资源池: 像计算、存储资源一样的安全服务资源

新增租户

1.租户信息 >>

租户名称:

密码:

确认密码:

手机号:

电子邮箱:

公司名称:

联系地址:

新增租户

1.租户信息 >> 2.选择安全服务包

安全服务包

☒ 服务包名称1

☐ 服务包名称2

☐ 服务包名称3

☐ 服务包名称4

☐ 服务包名称5

新增租户

1.租户信息 >> 2.选择安全服务

安全服务

安全接入

应用交付

安全运维

基础防御

新增租户

1.租户信息 >> 2.选择安全服务

根据您选择的安全服务

☒ 手动设置 ☐ 自动设置

安全接入:

应用交付:

安全运维:

基础防御:

新增租户

1.租户信息 >> 2.选择安全服务 >> 3.授权 >> 4.配置安全组件IP >> 5.预览所有配置

租户名称: 北京财政局

手机号: 122 3231 2132

电子邮箱: bjczj@163.com

公司名称: 北京财政局

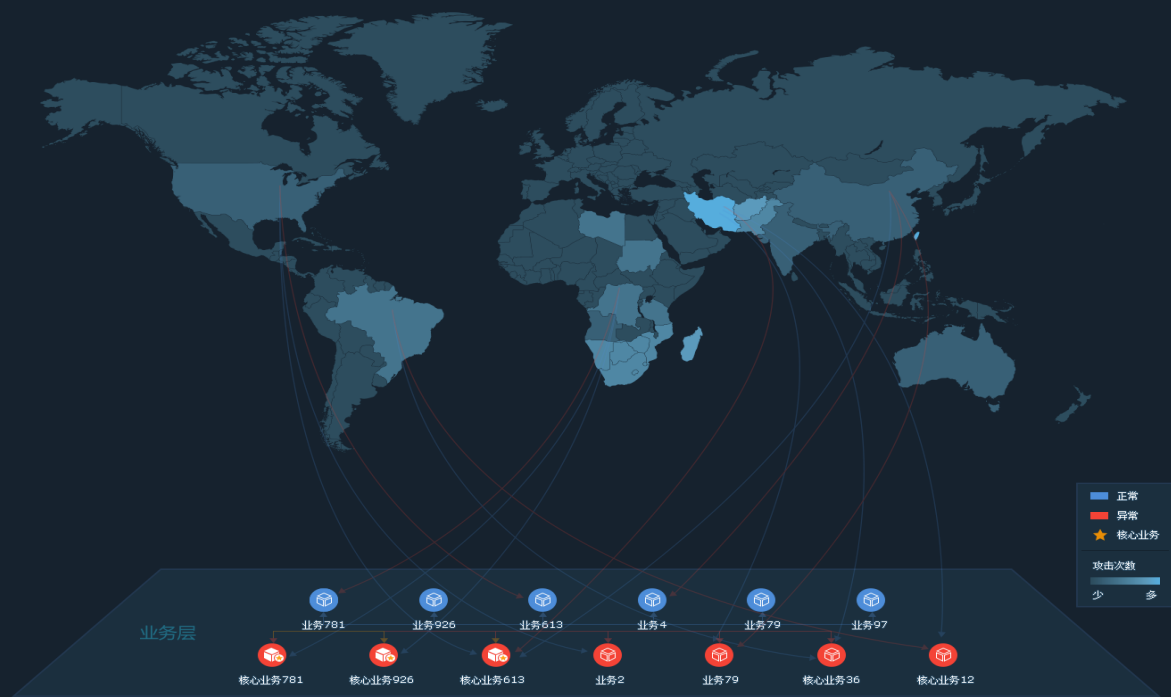
联系地址: -

安全接入	服务包1	50M	1年	200.200.1.111
应用交付	服务包1	100并发	6个月	200.200.1.112
安全运维	服务包1、服务包2	50M	1年	200.200.1.113
基础防御	服务包2	50M	1年	200.200.1.114

上一步 保存



实时流量可视



实时攻击流量

时间	源 IP 地址	源区域	资产	流量大小	应用	攻击类型
09-29 22:31	220.163.187.231	中国·广东	200.200.0.20	10.7mb/s	HTTP 应用	-
09-28 21:31	166.222.83.148	中国·上海	200.200.1.19	12.7mb/s	远程登录	-
09-27 20:31	212.125.138.112	美国	200.200.39.12	9.3mb/s	代理工具	SQL 注入
09-26 19:31	220.163.187.231	日本	100.110.212.5	7.6mb/s	网络流媒体	-
09-25 18:31	166.222.83.148	巴西	100.110.212.6	19.8mb/s	木马控制	-
09-24 17:31	212.125.138.112	新加坡	100.110.212.7	21.6mb/s	网络流媒体	SQL 注入
09-23 16:31	218.222.36.123	韩国	100.110.212.8	3.2mb/s	远程登录	xss 攻击



攻击源地区 TOP5

中国·广东	31924
新加坡	21514
日本	12436
韩国	9814
巴西	5536

SSL VPN

状态

+ 添加

编辑

☐ 名称

☒ 从人员管理系统

☐ 企业服务网系统



扫码观看大会视频

生态运营、开放共赢

云
服
务
商

联合运营

政务云
行业云
云化IDC
.....

云安全资源池

开放的安全服务APP Store

运维审计
SOC
威胁情报
.....

共建生态

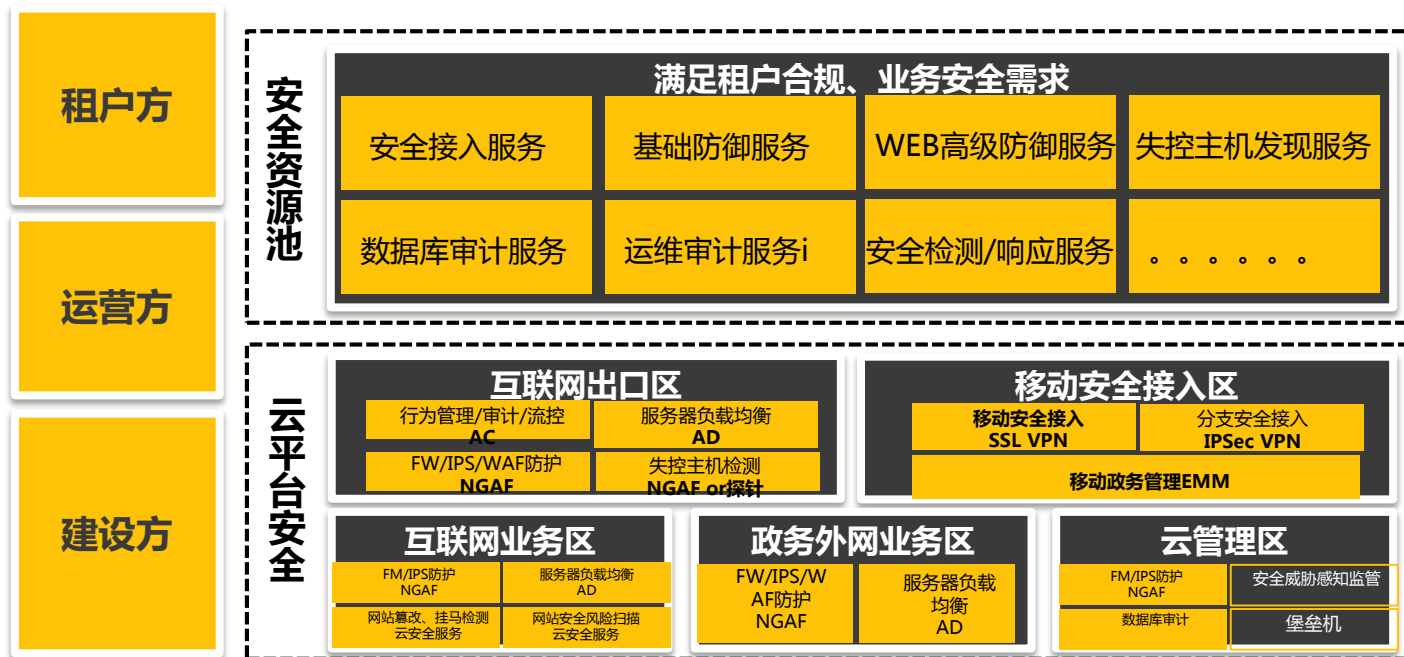
安
全
厂
商



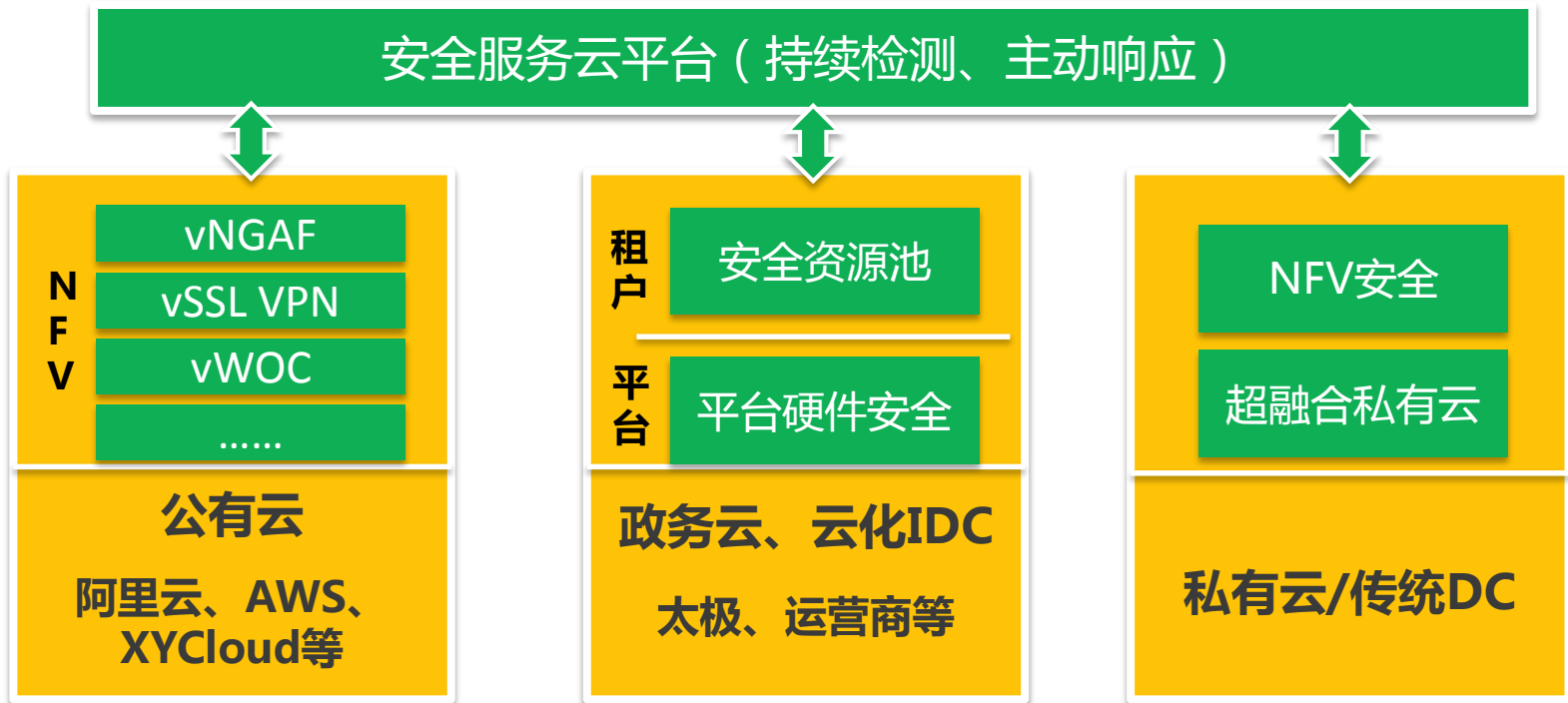
扫码观看大会视频

完善的政务云安全方案

让租户安全快速上云，让运营方业务不断增值



为用户构建跨云的安全能力



深信服技术能力表现

Magic Quadrant

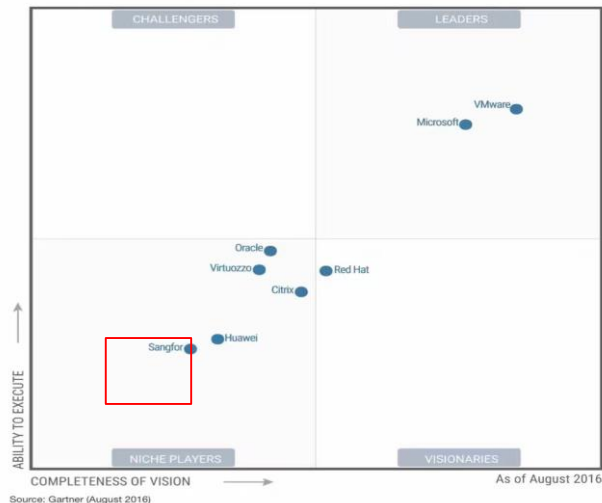
Figure 1. Magic Quadrant for Enterprise Network Firewalls



安全市场

Magic Quadrant

Figure 1. Magic Quadrant for x86 Server Virtualization Infrastructure



虚拟化市场



扫码观看大会视频

2016 The
Computing
Conference
THANKS

