The 8th China Cloud Computing Conference

第八届中国云计算大会

技术融合 应用创新

云环境下的企业安全策略

马元骐 (mma@paloaltonetworks.com)

Palo Alto Networks 亚太区数据中心、虚拟化及云顾问工程师

网络安全*已不再仅仅只是技术问题……*

什么正在变化？

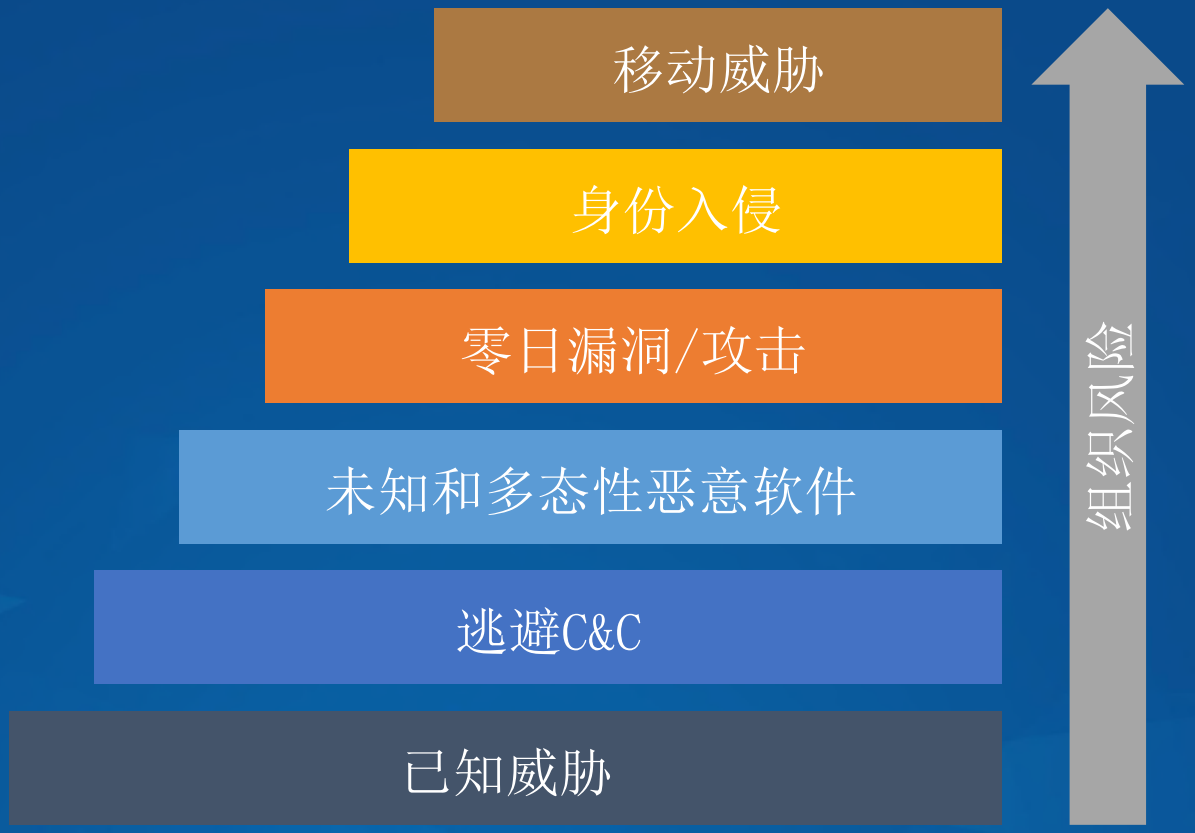
网络攻击者的进化

网络犯罪现状
市场规模达4450亿美元

网络军备
100+国家参与

什么正在变化？

网络攻击者的进化



“我把秘档埋进了办公室后面的咖啡罐子里，你那电脑是绝对入侵不了的”

公司数据 成为攻击目标

1,541

2014年报道的数据泄露事件

1,023,108,267

全球损失记录

32

每秒发生的事件

ttp://breachlevelindex.com/pdf/Breach-Level-Index-Annual-Report-2014.pdf

IT 和CIO 所扮演的角色在不断变化

IT一定要成为
实现战略商务的推动者

SaaS

webex successfactors workday salesforce jive

社交 + 消费化

Gmail LinkedIn EVERNOTE box facebook skype

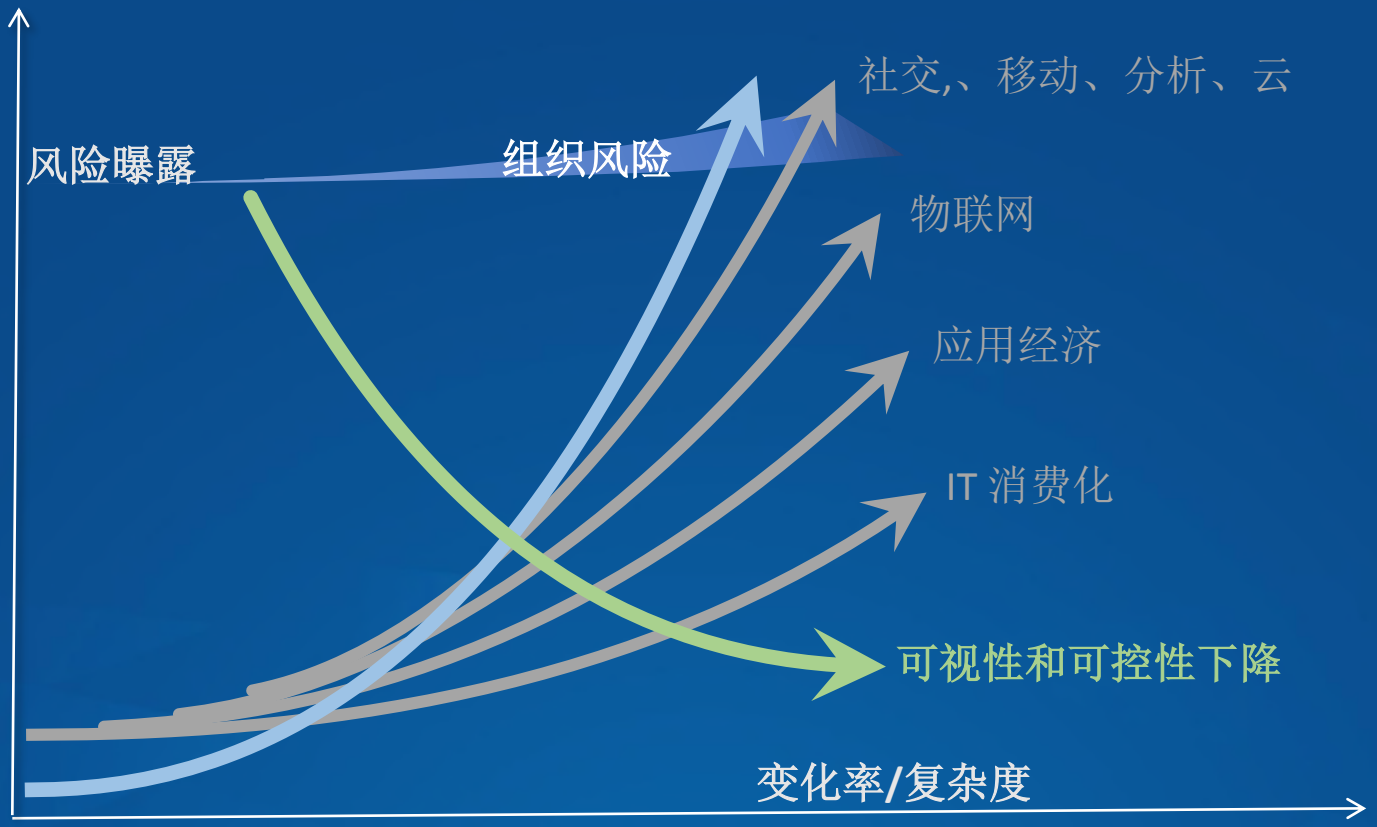
是机遇，还是挑战？

移动 + BYOD

云+ 虚拟化

商业结构的改变
将高级网络威胁带入了全新时代

挑战与改变，带来巨大风险



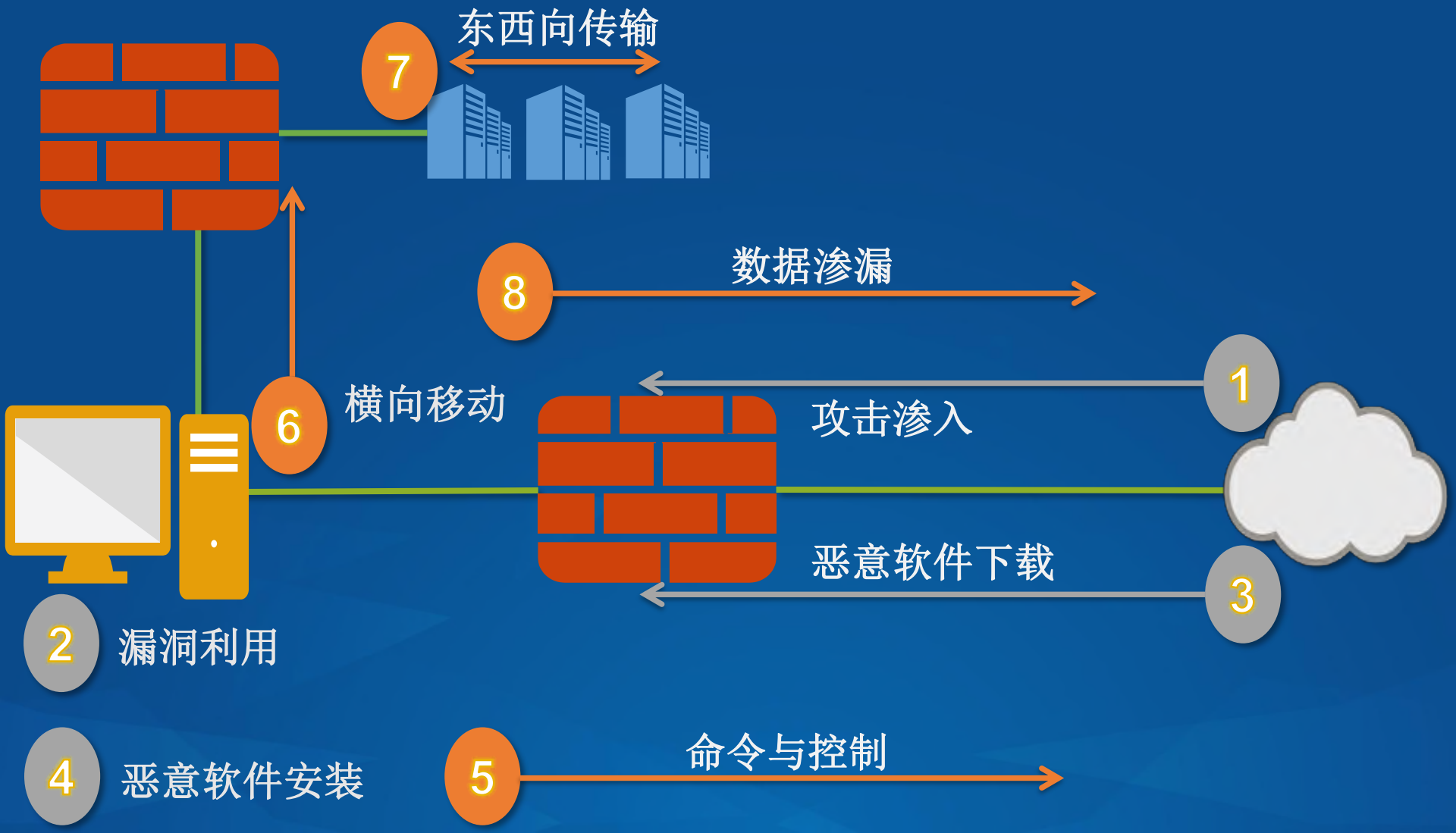
对服务提供商的多层依赖

深入了解攻击生命周期

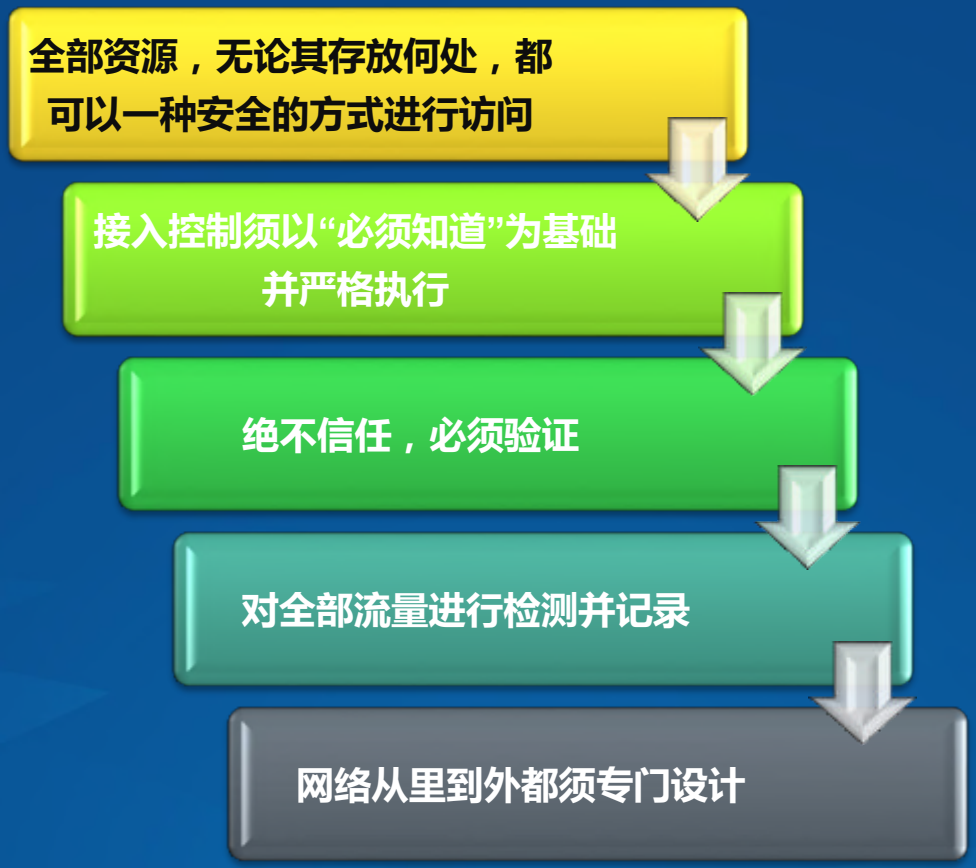
攻击生命周期

阻止攻击生命周期中的某一环节，便可阻止攻击的发生

攻击生命周期里面的防御时机



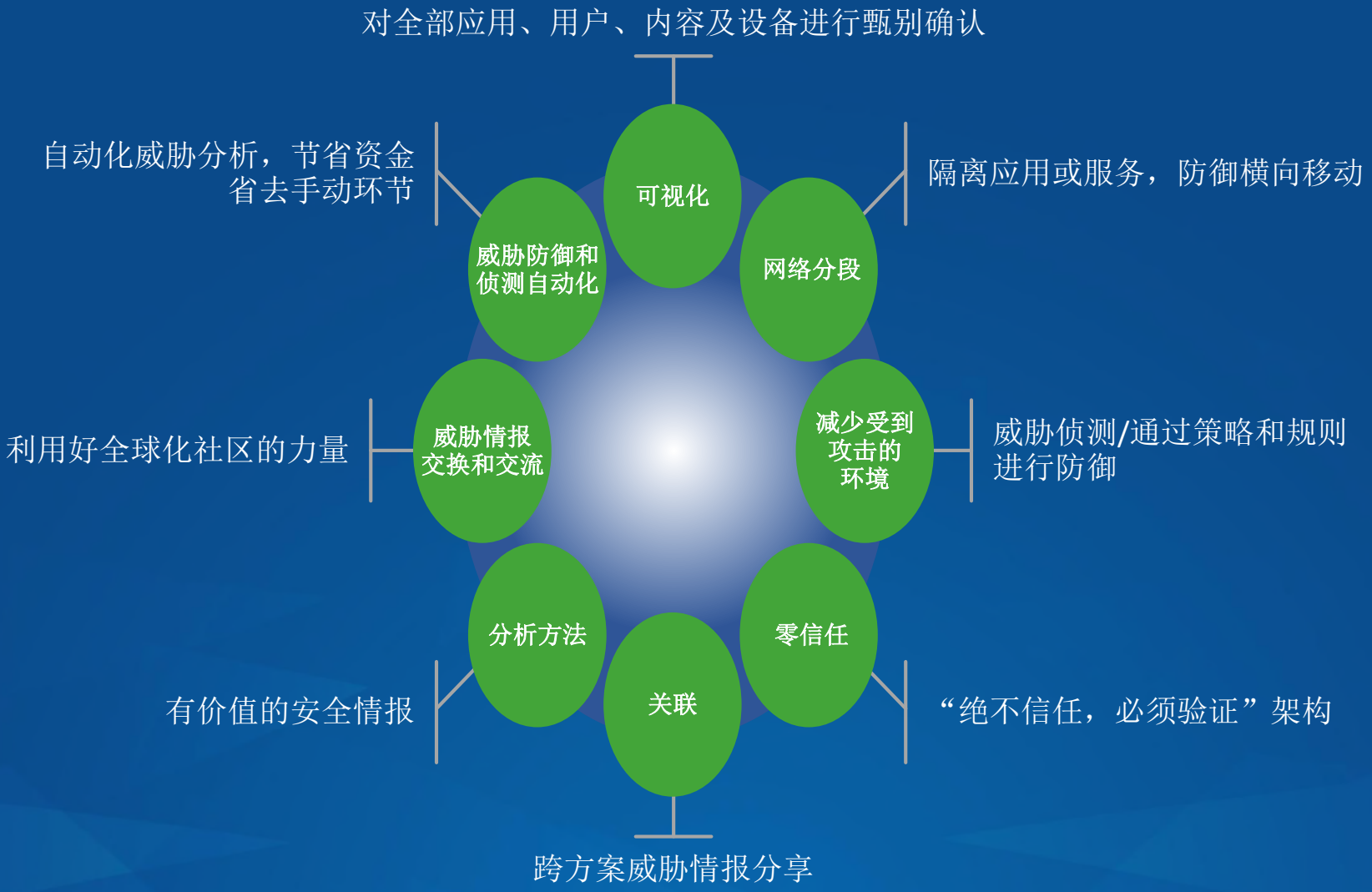
“零信任”的概念

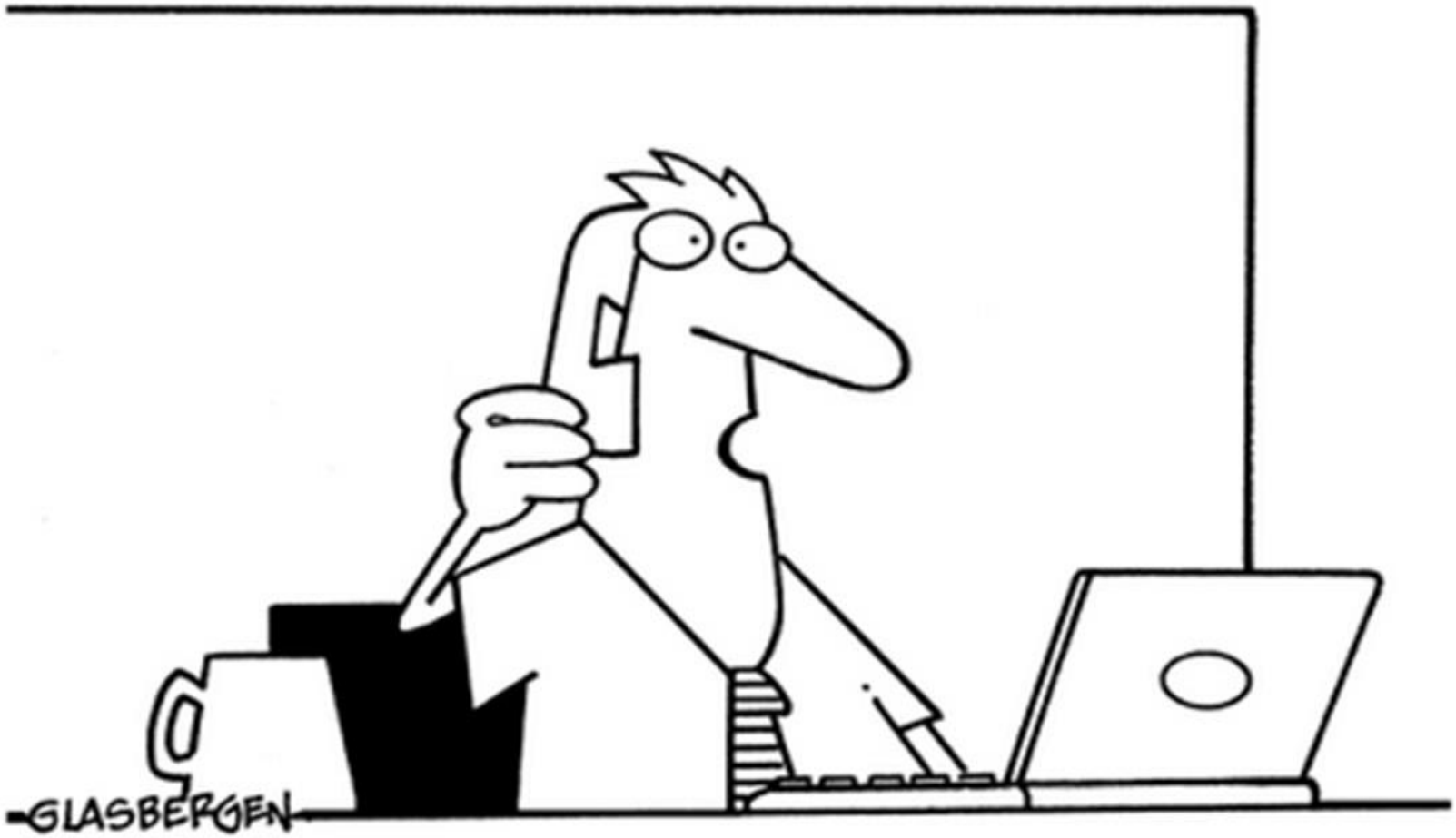

全部资源，无论其存放何处，都
可以一种安全的方式进行访问
接入控制须以“必须知道”为基础
并严格执行
绝不信任，必须验证
对全部流量进行检测并记录
网络从里到外都须专门设计

提高可视性，减少发生攻击的条件

- 借助领导力，确认何为合法应用并定义之
  - 调整安全策略，适应政府和商业应用
  - 隔离关键内部应用
  - 确定那些可以保护云与虚机用例的策略
- 将应用与用户/群组实现关联

高级安全方法


对全部应用、用户、内容及设备进行甄别确认
可视化
隔离应用或服务，防御横向移动
网络分段
减少受到攻击的环境
威胁侦测/通过策略和规则进行防御
零信任
“绝不信任，必须验证”架构
关联
跨方案威胁情报分享
分析方法
有价值的安全情报
威胁情报交换和交流
利用好全球化社区的力量
威胁防御和侦测自动化
自动化威胁分析，节省资金省去手动环节



“你确定我们在云上的数据就是安全的？

我怎么刚才在天气频道上看到了我做的表格“

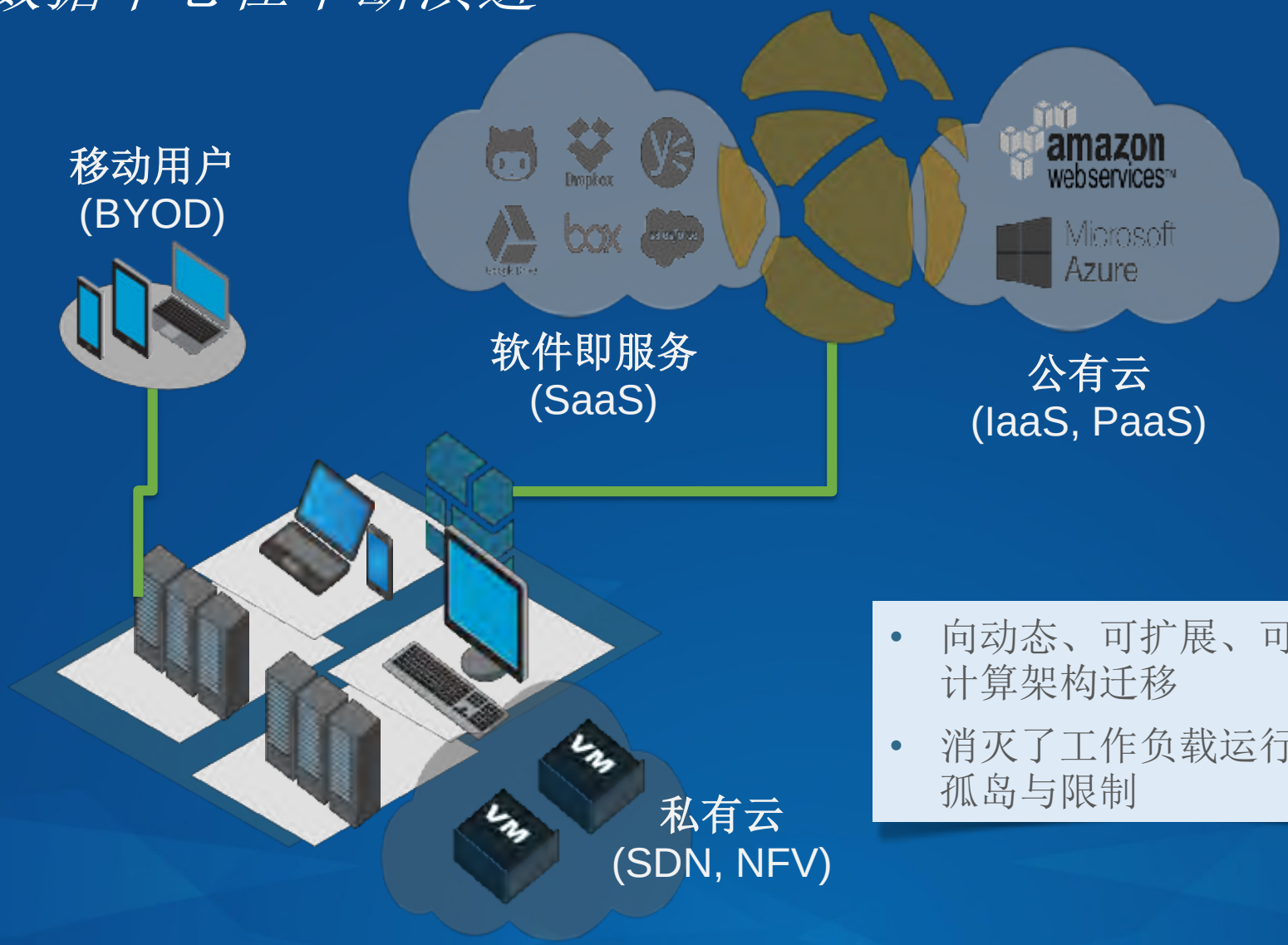
云安全挑战

有限可视性

技术落后，不连贯

流程冗长

数据中心在不断演进



- 向动态、可扩展、可自行配置的计算架构迁移
- 消灭了工作负载运行所需的计算孤岛与限制

安全：共同的责任

客户内容

平台、应用、身份与接入管理

操作系统、网络与防火墙配置

密钥管理 | 客户与服务器加密 | 网络流量保护

客户对其在云中的安全负有不可推卸的责任

amazon web services

Microsoft Azure

云基础设施与服务

计算 | 存储 | 数据库 | 组网

提供商负责照看云的安全

数据中心安全需求

安全

- 以“零信任”为原则使用和保护应用
- 防御任何已知和未知威胁
- 实现从实体机到虚机的安全一致性

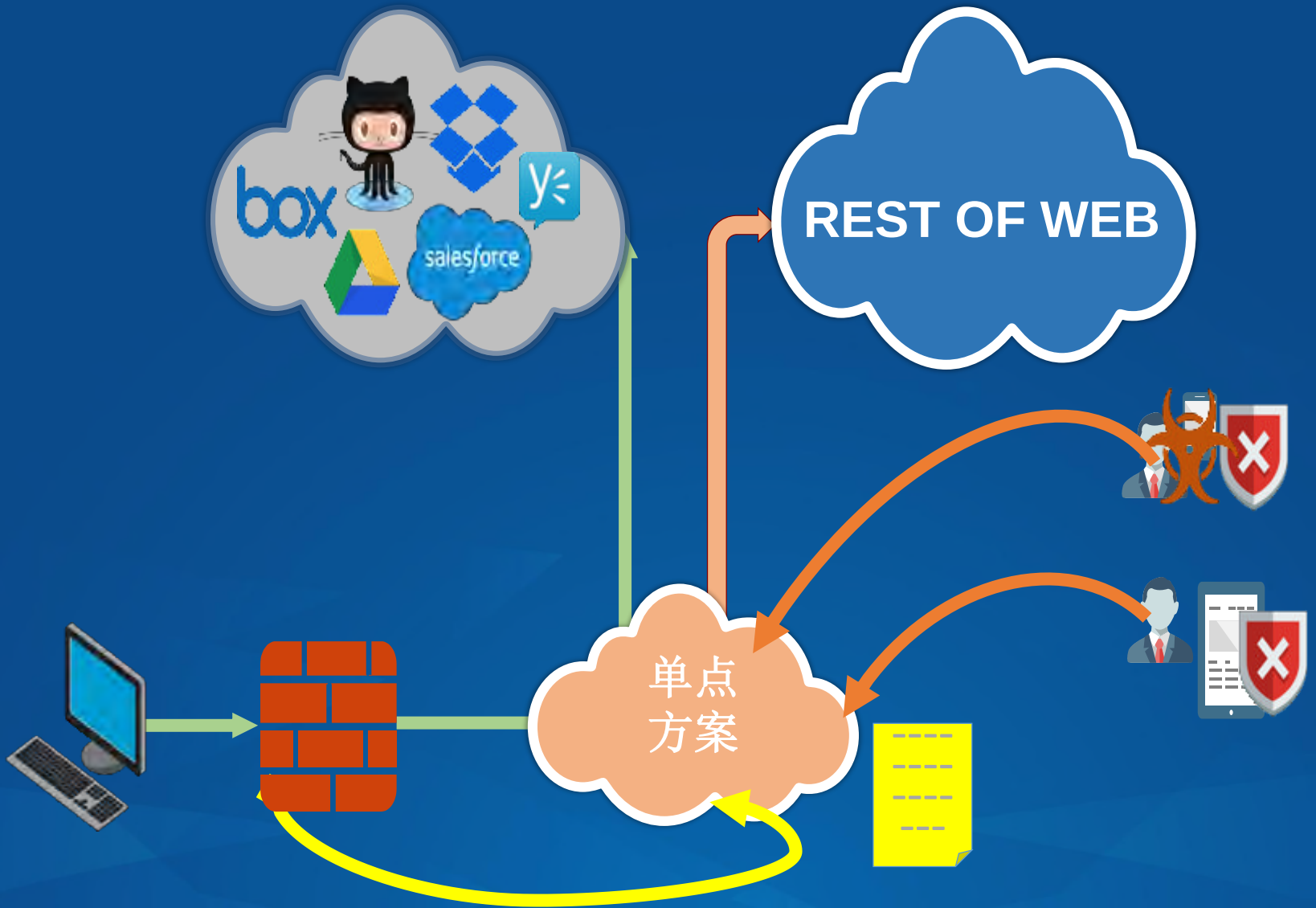
敏捷

- 在lock-step中对新工作负载进行安全配置
- 借助动态策略更新实现策略管理自动化
- 提供广泛的 hypervisor 环境支撑

迅速

- 提供可预见的 L7 分级和解析
- 可智能扩展至 200Gbps
- 简化管理和网络集成

现有的SaaS单点解决方案



确保SaaS安全的整体方法

下一代防火墙平台

发现
SaaS 应用的使用情况与统计数据

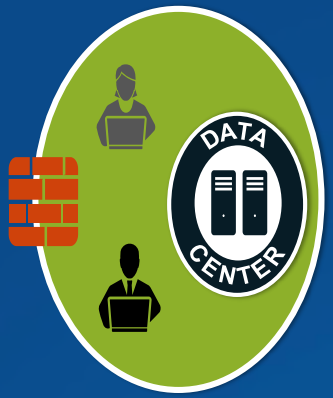
SAAS 接入
SaaS应用的接入与接出

云方案

SAAS 控制
数据曝露与威胁防护

安全需求，无处不在

移动终端



互联网边缘

局域网中员工和设备之间

数据中心边缘以及各虚机之间

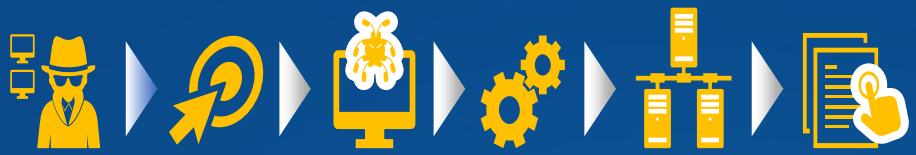
私有云、公有云、混合云以及SaaS之间

检测阻止企业中任意节点的威胁

主动分析威胁情报并参与情报交换

情报收集和分析

受损指示器



威胁

- 网络间谍
- 网络犯罪
- 网络黑客行为
- 网络军备
- 网络恶作剧
- 网络恐怖主义

威胁情报交换

APTA　ES-ISAC　FINANCIAL SERVICES　Microsoft

MARITIME ISAC　STANDARDS

NCC　NEI　STIX　TAXII

网络安全的明天

- 实现对全网以及深入“云”内部的可视化和检测
- 网络分段与微分段
- 高级安全可防御安全指示器以及攻击生命周期
- 移动和BYOD 安全
- 物联网和嵌入式终端设备安全
- 高级分析方法和大数据安全分析
- 像国际刑警组织那样，实现对高级威胁和活动情报的互通有无
- 高级安全新技术，如：Apple采用tokenization 技术来消除CC#通信和存储隐患

The 8th China Cloud Computing Conference

Thank you