

**RSA[®]CONFERENCE
C H I N A 2012
RSA信息安全大会2012**

**THE GREAT CIPHER
MIGHTIER THAN THE SWORD
伟大的密码胜于利剑**



新的安全威胁态势下 企业安全架构的重塑

马蔚彦

赛门铁克（软件）北京有限公司



RSA CONFERENCE
C H I N A 2012
RSA信息安全大会2012

推动企业安全建设转变的动态环境

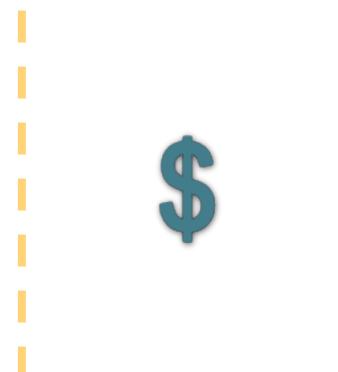


2011年重要数字：揭示三大威胁趋势

55亿次	赛门铁克拦截的攻击		+81%
4.03亿个	恶意软件的特殊变体		+41%
4597次	每日网页攻击		+36%
110万个	单次身份泄露数量		+323%
315个	新移动设备漏洞		+93%

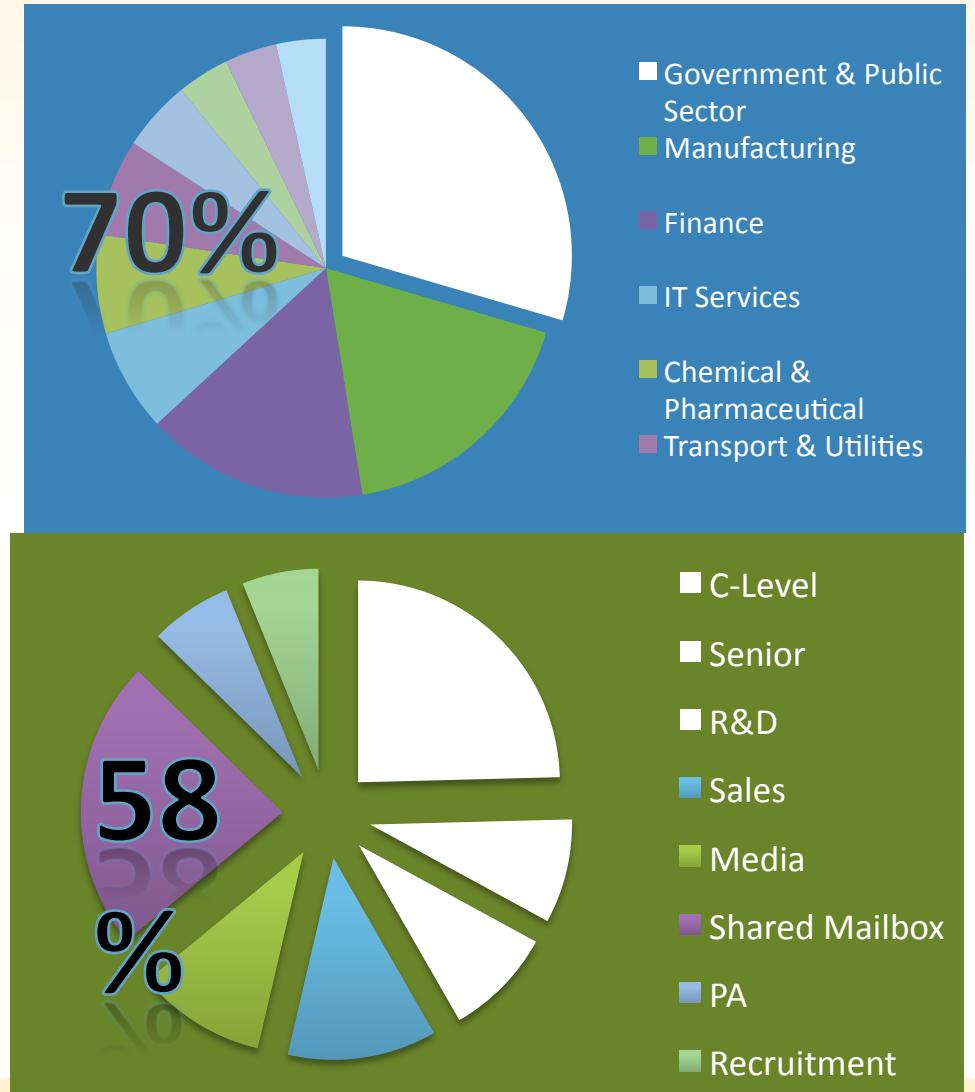
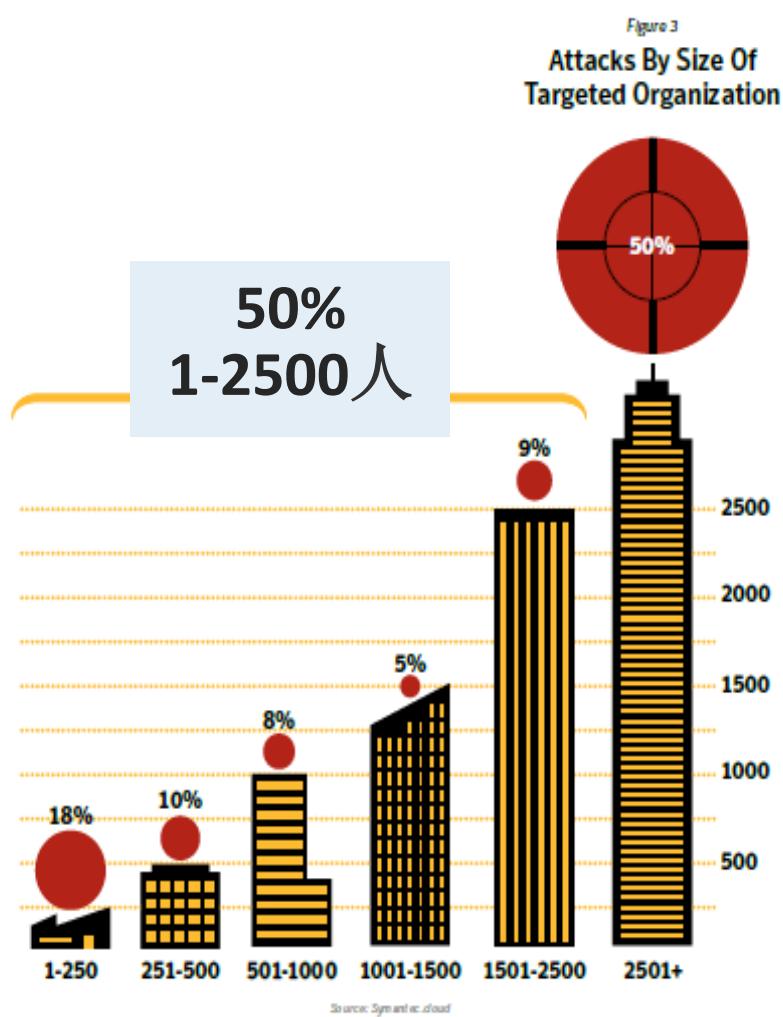
趋势1：恶意软件攻击持续快速增长

$$\mathcal{A}^{\$} + \mathcal{U}^P = 5.5B$$

APT攻击蔓延—企业规模/人员/行业

RSACONFERENCE
C H I N A 2012



2011年重要数字：揭示三大威胁趋势

55亿次	赛门铁克拦截的攻击		+81%
4.03亿个	恶意软件的特殊变体		+41%
4597次	每日网页攻击		+36%
110万个	单次身份泄露数量		+323%
315个	新移动设备漏洞		+93%

趋势2：数据泄漏数量继续增加

- 2011年有**2.32亿个**身份被暴露。
- 单次数据泄漏损失达**550万美金***

2011年重要数字：揭示三大威胁趋势

55亿次	赛门铁克拦截的攻击		+81%
4.03亿个	恶意软件的特殊变体		+41%
4597次	每日网页攻击		+36%
110万个	单次身份泄露数量		+323%
315个	新移动设备漏洞		+93%

趋势3：企业和个人用户面临移动威胁

推动企业安全建设转变的动态环境

RSACONFERENCE
C H I N A 2012



IT基础设施的三大转变

虚拟化, 云, 移动 (Virtualization, Cloud, Mobility)

RSACONFERENCE
C H I N A 2012

数据中心



受管理的设备



虚拟数据中心

(Virtualized Data Center)



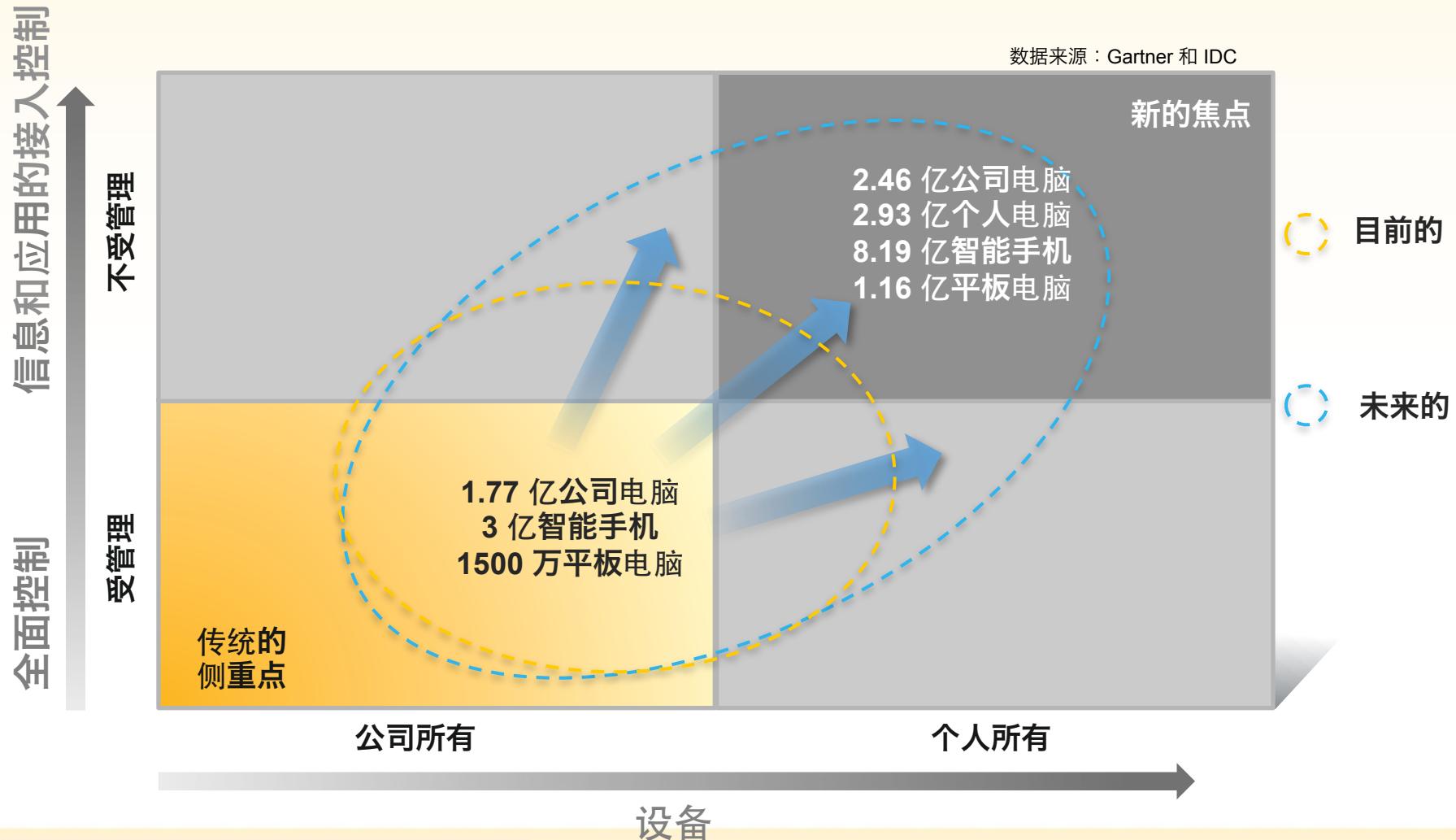
云



不受管理的设备



企业移动应用的趋势



IT基础设施三大转变-带给企业的困境



以其提高生产力而必须支持 (Must support to enhance employees productivity)



困境



无法应付众多平台的信息保护、安全风险及合规问题 (*I do not have the means to control security, risk, and compliance across all of these new I.T. platforms*)

Private Cloud

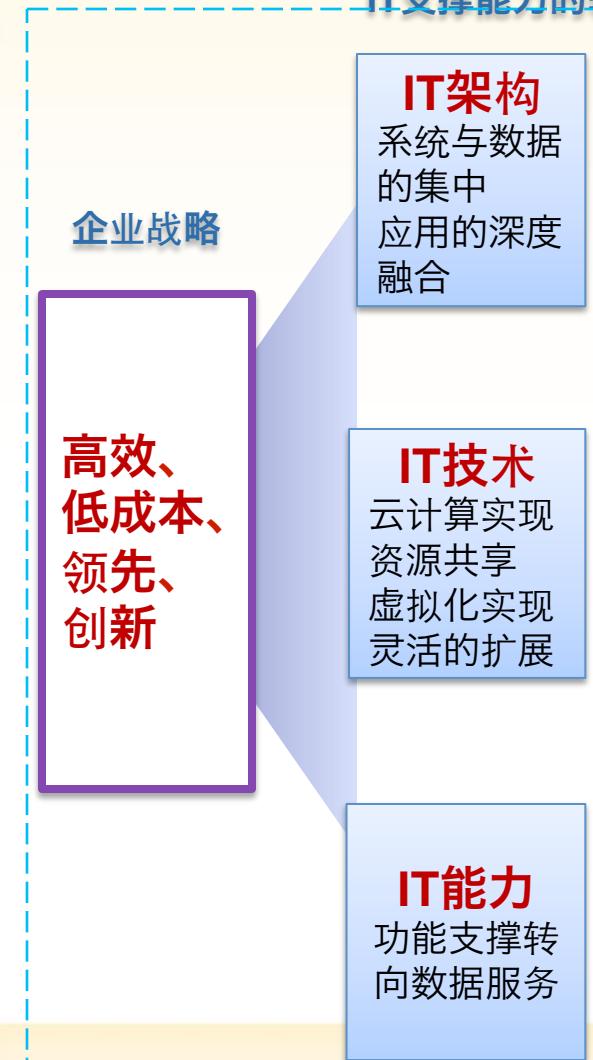


Cloud



以其提高业务的灵活性和降低成本而成为必然 (Must embrace to drive business agility and lower costs)

IT支撑能力的转变促成安全建设方向的调整

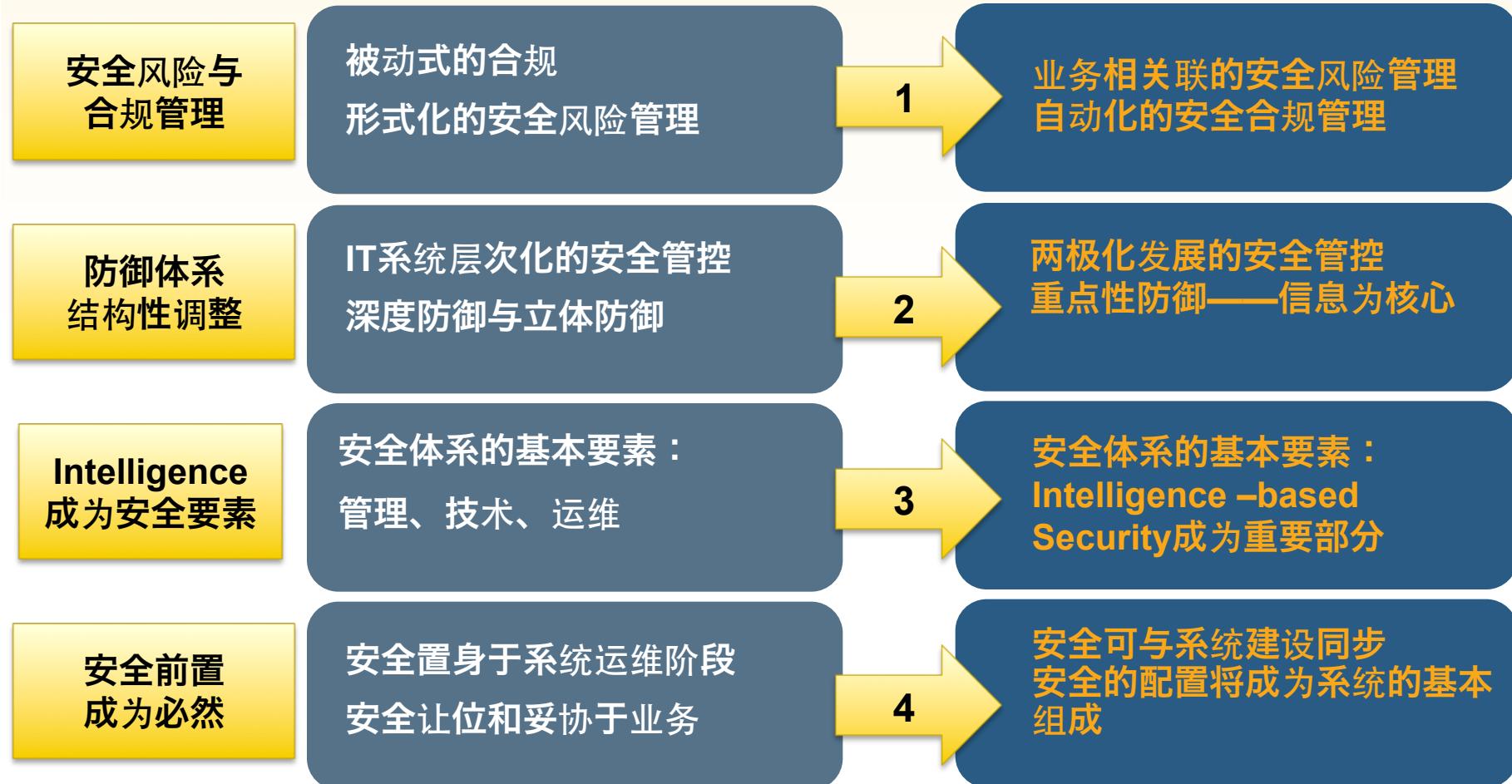


推动企业安全建设转变的动态环境

RSACONFERENCE
C H I N A 2012



企业安全建设正经历着4个重要转变



安全风险与 合规管理

被动式的合规
形式化的安全风险管理

1

业务相关联的安全风险管理
自动化的安全合规管理

自动化与业务化的风险与合规管理

风险管理的业务相关性需求得到推动



- data breaches and **early evidence of the breach in the log record 90% of the time**, but the companies involved noticed it only **5% of the time**.
----“2010 Data Breach Investigations Report” conducted by the Verizon Business RISK Team

- **定向攻击成为趋势之前**：依托周期性的威胁和漏洞发现，以及半工具半人工方式的漏洞弥补，是可接受的风险管控方式。业务相关性的要求并非必要。
- **定向攻击的蔓延和扩散**：潜伏越久，损失越大。使得及早发现威胁，及时采取措施降低风险，及时对执行情况核查逐渐成为刚需。同时，业务相关性成为必须。

解决企业在IT风险管理中的难题与关键

1

可视化

- 把IT风险的影响以业务相关的方式来表达
- 带动安全意识、所采取的行动以及责任
- 消除安全和IT操作之间的鸿沟

2

风险优先级

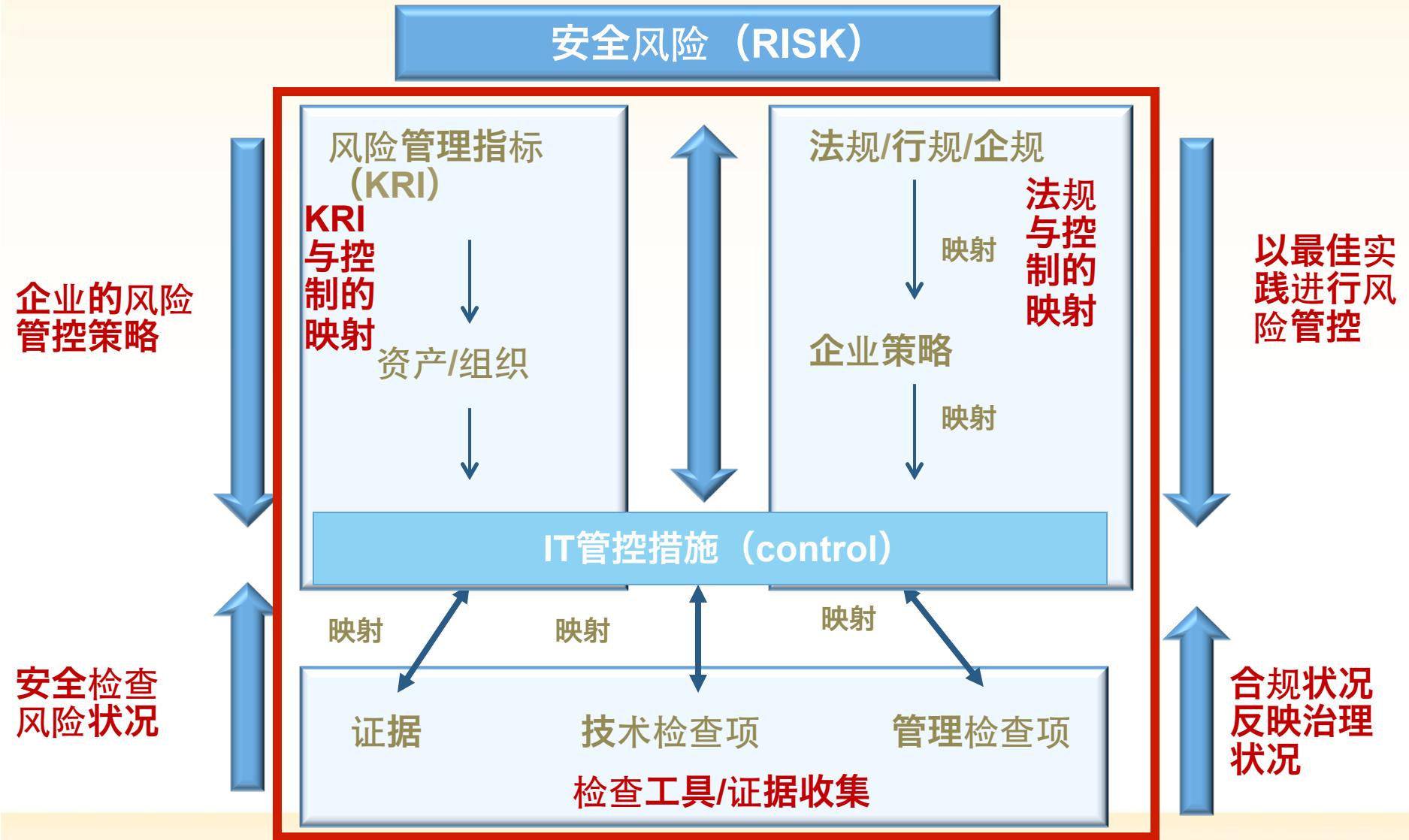
- 以数据推导出的结论更具备说服力
- 按照业务风险而不是技术优先级来对问题排序
- 优先解决最高级别的风险

3

自动化

- 自动化评估和修复
- 利用持续的评估获得更精确的数据
- 按特定需要提供自动流程化的响应的能力

关键技术—建立IT控制/风险/法规的映射



防御体系
结构性调整

IT系统层次化的安全管控
深度防御与立体防御

2

两极化发展的安全管控
重点性防御——信息为核心

两极化的安全管控，重点性的防御体系

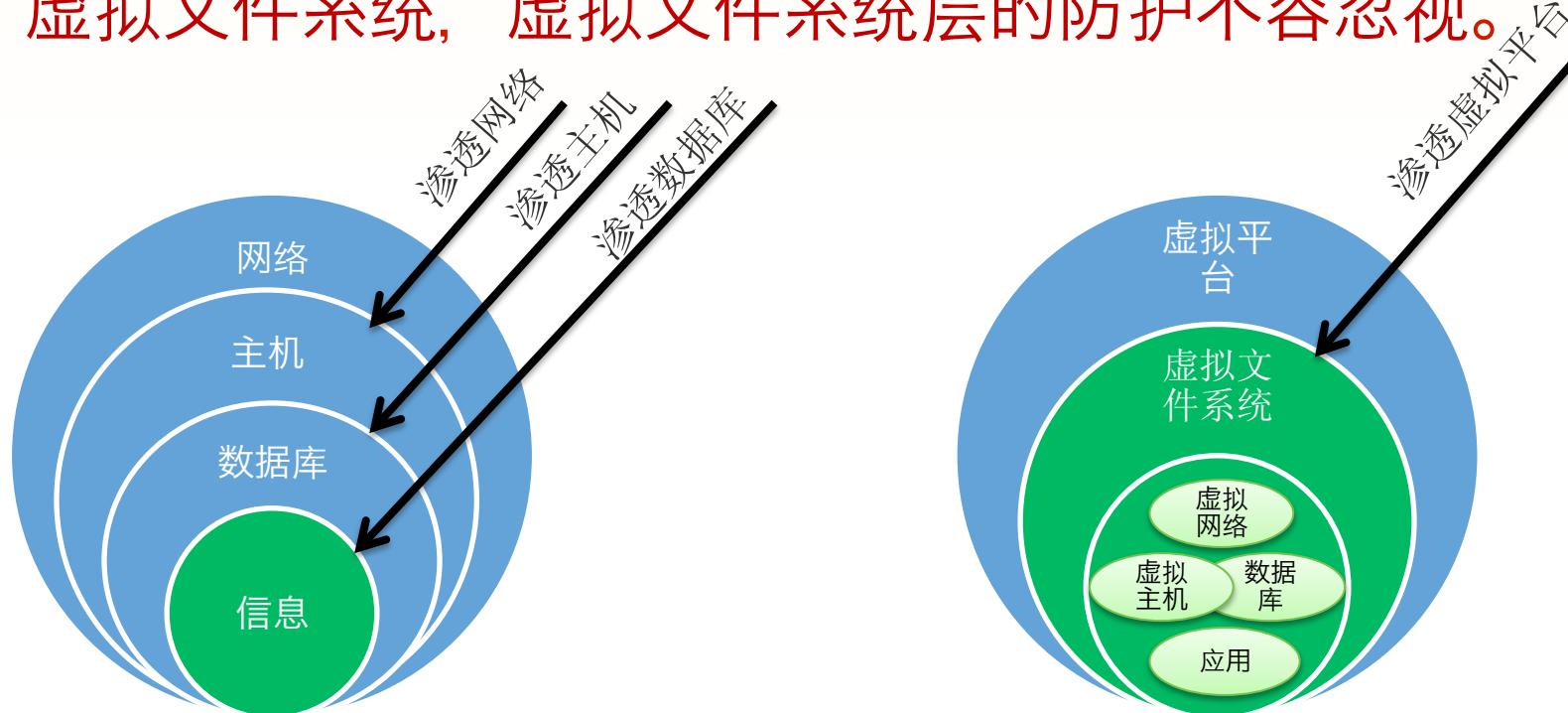
层次化与两极化的根本性变化—可控性

- 风险：控制力变弱，可视程度变弱
- 防御重点1：对物理资产的管控逐渐弱化
 - 实体资产位置、owner、责任主体变化和不受控
 - 加强和依赖SLA解决
- 防御重点2：对信息资产的管控强化
 - 实体资产（包括数据本身）有可恢复性
 - 信息的损失难以弥补



云端——虚拟平台安全成为新焦点

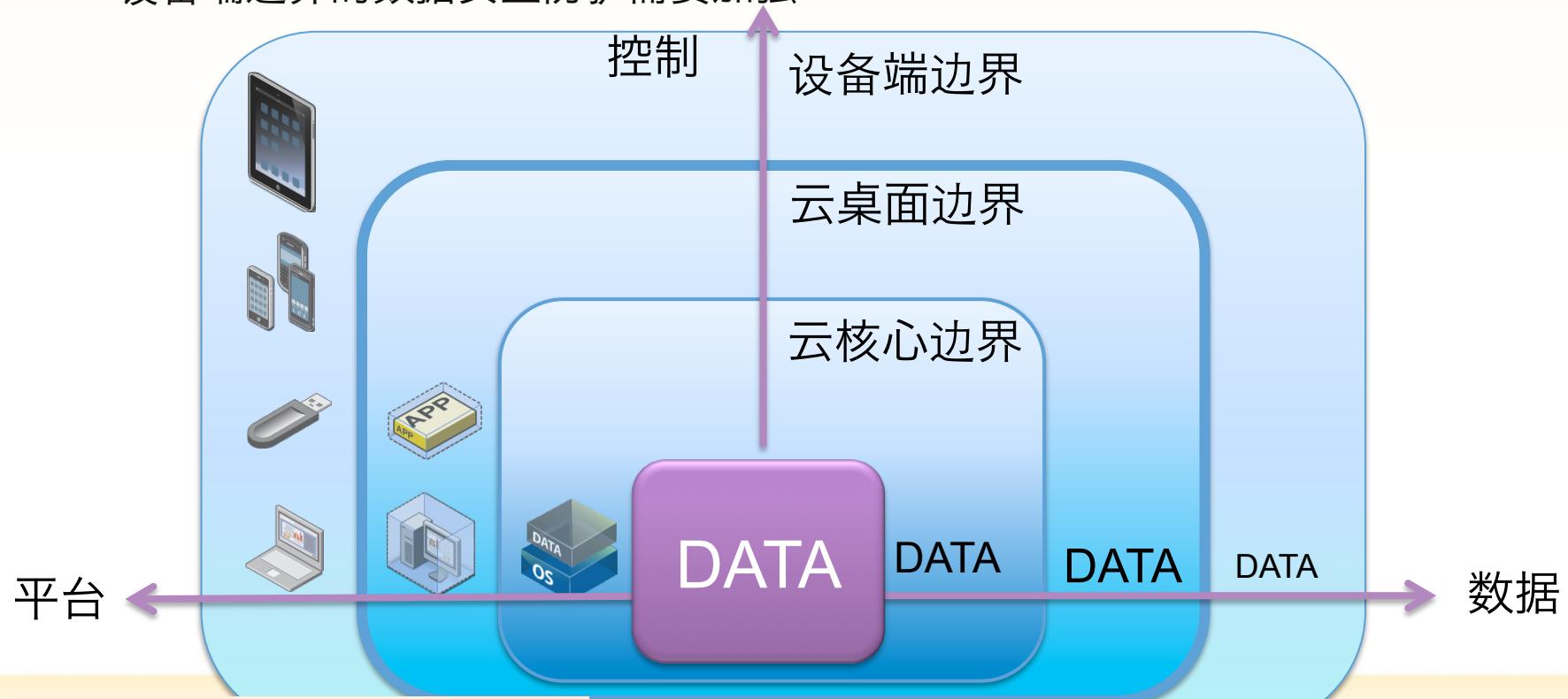
- 传统数据中心，业务数据大多保存在结构化系统中，要获取数据需要多层授权控制，并通过复杂的查询过程进行，受控程度高
- 虚拟化平台下，信息承载和存在形式从数据库变成了虚拟文件系统，虚拟文件系统层的防护不容忽视。



云端（私有云）—数据的安全边界变化

RSACONFERENCE
C H I N A 2012

- 原边界：安全域、系统域（以系统为核心的视角），以网络层次、功能、业务重要性为划分依据
- 新边界：基本单位收敛到了主机或虚机（网络边界模糊化，动态资源分配）
终端虚拟化，使数据不落地，高敏感数据集中在服务端侧
设备端边界的 data 安全防护需要加强



设备端——BYOD管控重点的变化

RSACONFERENCE
C H I N A 2012

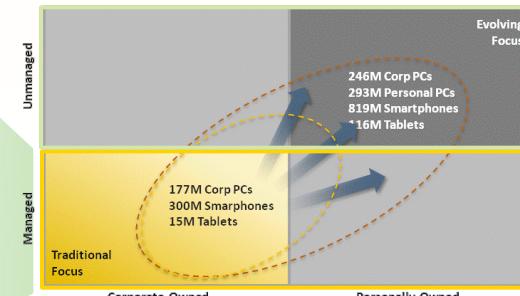
从关注企业受管设备的基础安全、数据保护；
到更关注BYOD的个人/企业应用及数据的分离与独立保护

企业受管设备

遵从性管理

基础安全策略管理

数据独立性



个人拥有设备

数据必须被独立保护

应用程序之间的数据
必须安全

企业和个人应用必须
分隔开

可管理设备



安全的程序以及数据



云环境安全防护新方法—“云外云” (O₃-Cloud Firewall)



Intelligence成
为安全要素

安全体系的基本要素：管理、
技术、运维

3

安全体系的基本要素：
Intelligence –based
Security成为重要部分

智能化安全 (Intelligence-based Security)

云计算对于安全的重大创新 —安全资源的集中化

RSACONFERENCE
C H I N A 2012

- 云服务的方式提供安全的能力
- 安全资源集中化的优势
 - 更好地感知安全态势（提供预警）
 - 大量知识的聚合（应对新威胁趋势）
 - 广泛的可操作的资讯和知识库
 - 更专业化、全面性的安全支持

赛门铁克全球智能网络 (Global Intelligence Network)

Identifies more threats, takes action faster & prevents impact



Worldwide Coverage

Global Scope and Scale

24x7 Event Logging

Rapid Detection

Attack Activity

- 240,000 sensors
- 200+ countries

Malware Intelligence

- 133M client, server, gateways monitored
- Global coverage

Vulnerabilities

- 40,000+ vulnerabilities
- 14,000 vendors
- 105,000 technologies

Spam/Phishing

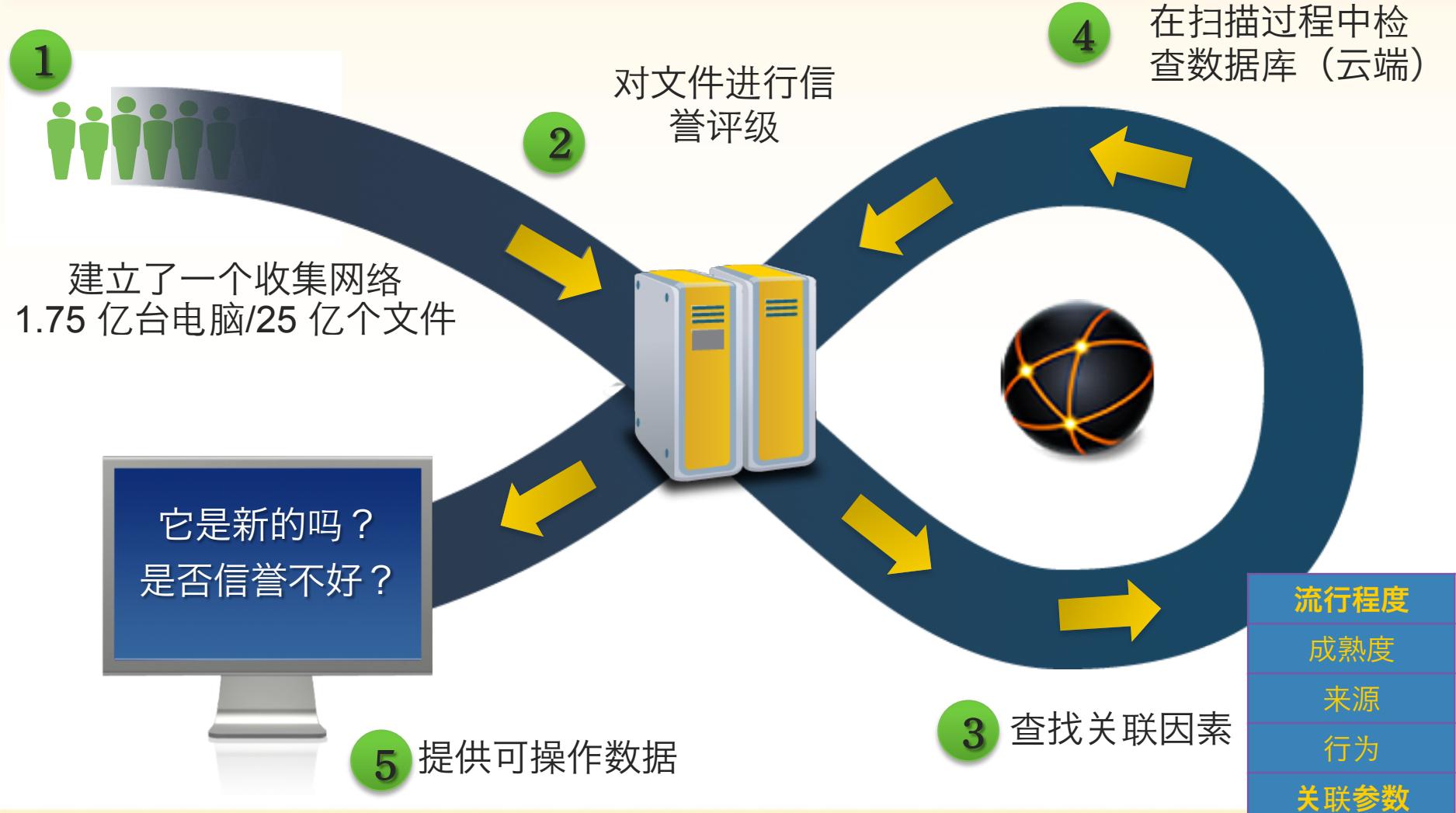
- 5M decoy accounts
- 8B+ email messages/day
- 1B+ web requests/day

Preemptive Security Alerts

Information Protection

Threat Triggered Actions

典型的云端信誉评级的技术



Intelligence在企业安全架构中的作用

- 原有架构中：
 - 安全知识库系统作为安全运维层面的一个静态知识库
- 未来架构中：
 - Intelligence融入技术体系（产品中）
 - Intelligence融入运维体系（及时的发现、响应机制、预警）
- Intelligence对企业安全建设的价值
 - 将成为安全体系架构中的重要组成
 - 下一代SOC系统的关键
 - 运用知识、贡献知识；更广泛的互动
 - 将企业个体安全与全球整体安全关联和结合

安全前置
成为必然

安全置身于系统运维阶段
安全让位和妥协于业务

4

安全可与系统建设同步
安全的配置将成为系统的基本组成

安全前置——真正实现全生命周期安全 (Lifecycle Security)

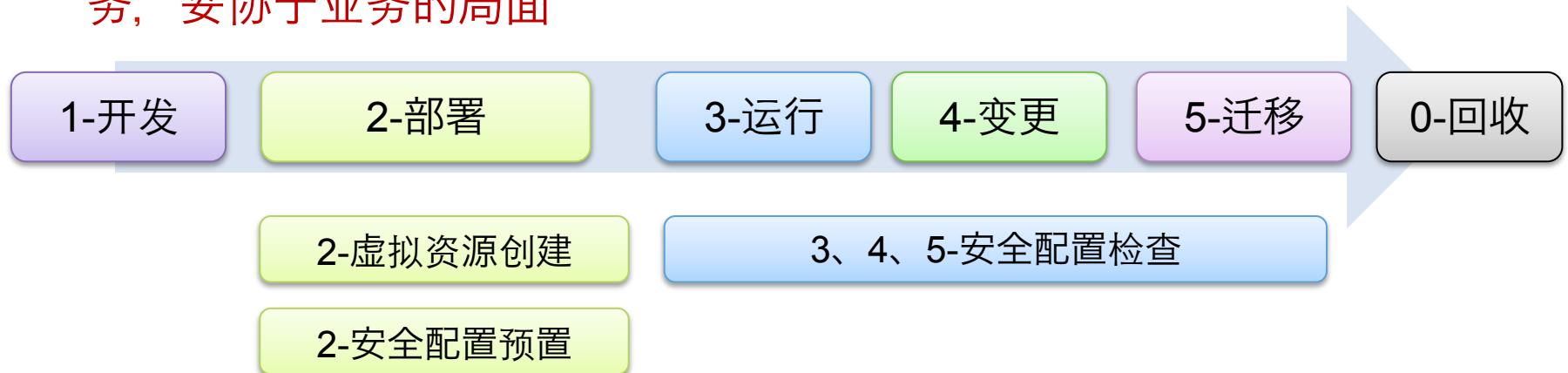
虚拟化技术—威胁快速扩散的根源

- 传统数据中心，安全问题分布在网络、系统、应用等各个层面，威胁的扩散依赖于威胁自身的传播能力，分而治之，扩散风险可控。
- 虚拟化平台下，带来了安全威胁的快速复制和扩散风险，比如Guest VM的镜像、拷贝、分发等，安全威胁可以从源头快速扩散。
- 安全工作必须从源头做起，如从Guest VM的创建做起。



虚拟化技术—安全前置成为可能和必须

- 系统生命周期缩短，系统上线与运维阶段的工作内容逐渐模糊，组织架构的不适应性，人员分工职责也出现模糊
 - 系统管理员、网络管理员分离
 - 二者模糊于虚拟平台管理员
- 安全工作置身于运维阶段的传统方式难以适应，虚拟化方式的资源管理使预置安全配置成为可能，并且成为必须。彻底改变安全让位于业务，妥协于业务的局面



未来5年企业安全架构重塑的战略及战术



谢谢



RSA CONFERENCE
C H I N A 2012
RSA信息安全大会2012

标题

- 第一条内容文字，微软雅黑，28号字
- 第二条内容文字
- 第三条内容文字
 - 二级内容文字，微软雅黑，24号字
 - 三级内容文字，微软雅黑，20号字