面向应用的混合云安全架构

臧铁军

VMware中国卓越中心
首席架构师

ISC 2017 中国互联网安全大会

360互联网安全中心

目录

- 云环境下的安全态势
- 面向应用的云安全架构
  - 打造安全生态体系，协力云安全
  - 基础架构安全治理，从被动到主动
  - 聚焦应用与数据，实现精准防护

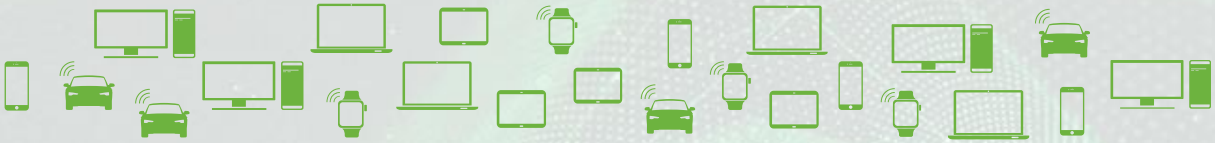
企业IT架构的全面转型

过去……

企业IT架构的全面转型

现在……

设备



应用

APP APP APP

传统应用

APP APP APP

云原生应用

SaaS SaaS SaaS

SaaS应用

基础架构

私有云

混合云

公有云

计算、存储、网络资源池化

安全仍然是上云的头号壁垒

采用云战略的壁垒

#1 一般安全风险 — 33%

#2 缺少经验 — 28%

#3 与现有IT环境集成 — 27%

#4 数据丢失与泄漏 — 26%

#5 法规遵从 — 24%

主要关注点

数据丢失与泄露 — 57%

数据隐私保护 — 49%

私密性 — 47%

法规遵从 — 36%

数据管理与控制 — 30%

Data from Cloud Research Partners https://dome9.com/wp-content/uploads/2017/03/Cloud-Security-Report-2017.pdf

2017年度信息安全领域热点技术

ISC 2017 中国互联网安全大会

360互联网安全中心

软件定义的边界
Software Defined Perimeters

云负载保护平台
Cloud Workload Protection Platforms

远程浏览器
Cloud Workload Protection Platforms

微分段
Microsegmentation

一体化运维安全
DevSecOps

端点检测与响应
Endpoint Detection and Response

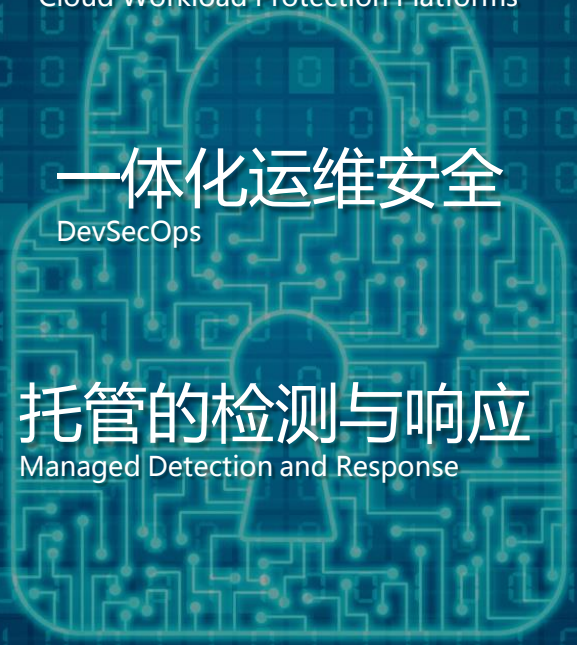
网络流量分析
Network Traffic Analysis

托管的检测与响应
Managed Detection and Response

云访问安全代理
Cloud Access Security Brokers

容器安全
Container Security

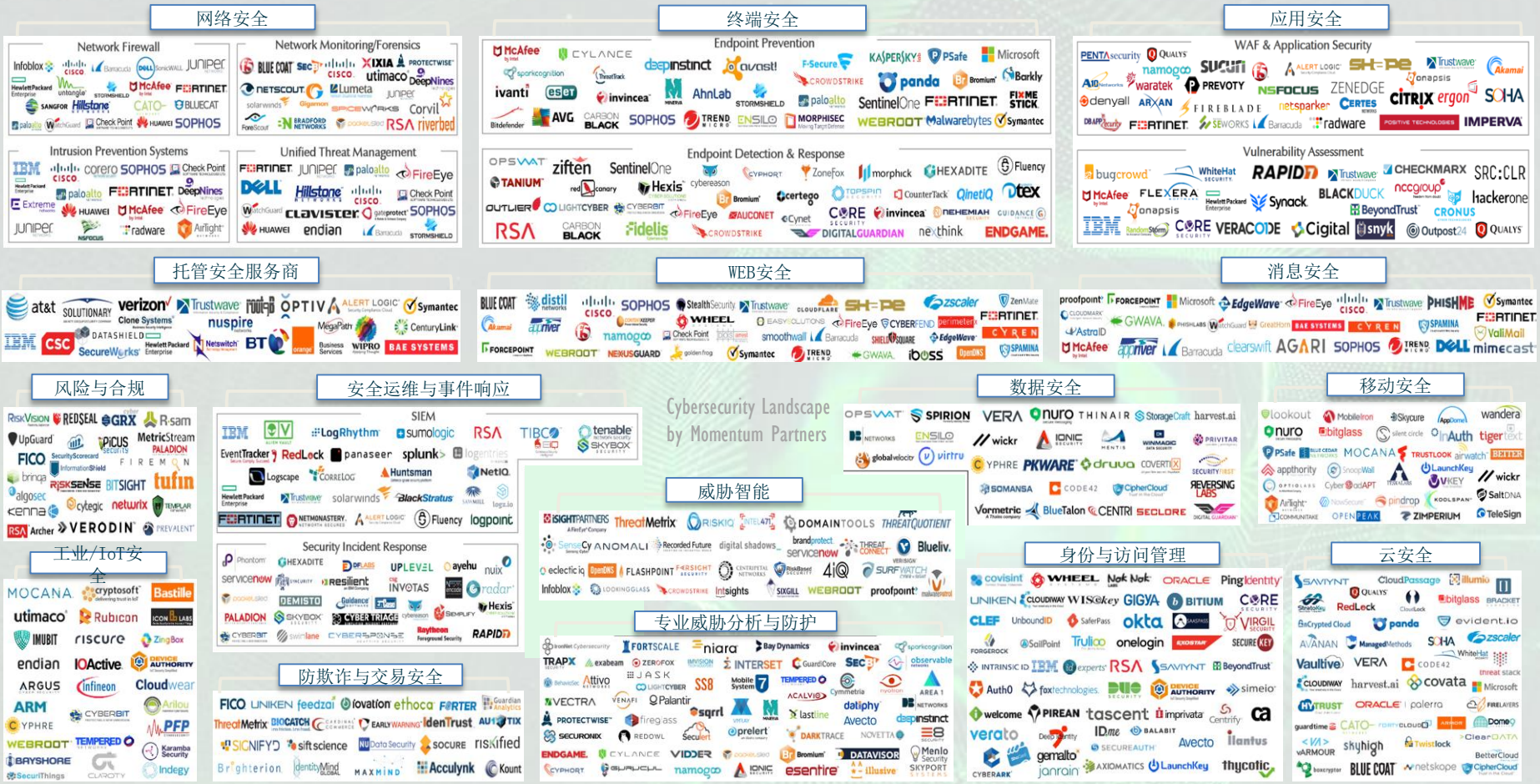
诱骗
Deception



信息安全市场的繁荣景象

ISC 2017 中国互联网安全大会 | 360互联网安全中心

更多选择→更多安全孤岛



转型到云安全

企业数字化转型

- 驱动业务创新 提升敏捷度
- 创建杰出的 移动性体验
- 保护品牌和 客户信任度

IT战略性任务

数据中心 现代化

集成 公有云

数字化 工作空间

转型到 云安全

我们致力于安全的集成与融合

策

安全策略

法律法规
安全标准与规范
最佳实践

咨询

术

攻防技术

监测
防御
修复

专业服务

阵

体系架构

平台建设
服务部署
交互

云架构

驭

安全管理

集成
自动化
可控

云管理

构筑云安全生态圈

识别 → 防护 → 检测 → 响应 → 修复

利用在虚拟化、移动性和混合云管理方面的核心能力实现无处不在的安全保护

ca

Check Point
SOFTWARE TECHNOLOGIES LTD.

FORTINET

HYTRUST
Cloud Under Control

intel Security

TREND MICRO

天融信 TOPSEC

Hillstone NETWORKS

paloalto NETWORKS

RAPID7

Symantec

f5

利用微分段实现零信任安全

入侵 → 渗透 → 破坏 → 撤出

入侵防范

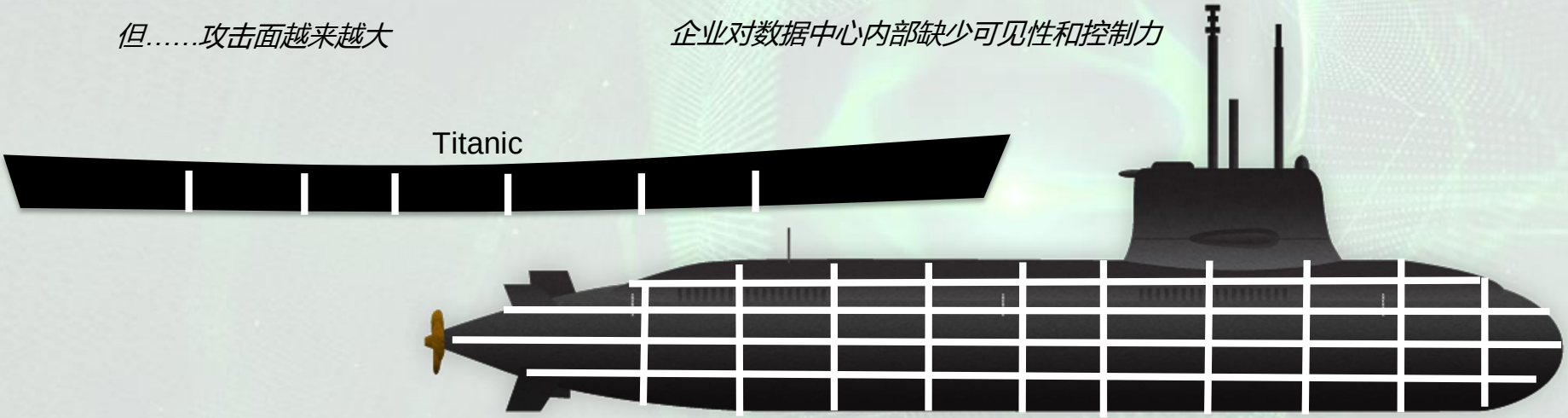
破坏防范

80%的投资用于防范入侵

但……攻击面越来越大

20%的投资用于防范入侵后行为

企业对数据中心内部缺少可见性和控制力



要确保一次成功的入侵不会将整个企业置于危险之中

无处不在的防护：NSX即服务

vmware®

ON PREMISES DATA CENTER

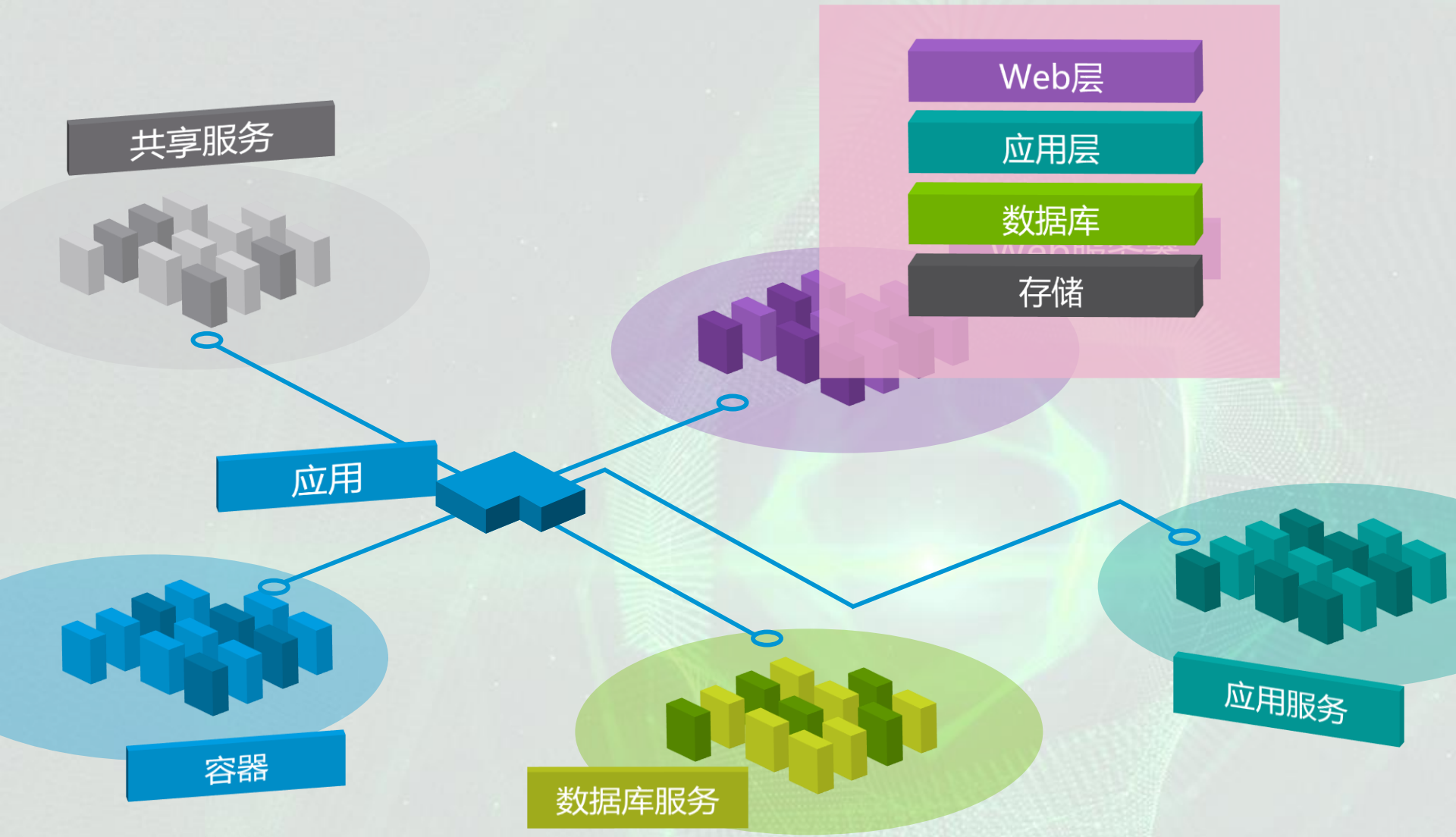
SOFTLAYER® an IBM Company

amazon web services™

Microsoft Azure

Google Cloud Platform

分布式架构的安全成本



云环境下的安全运维

DAY 2
安全运维

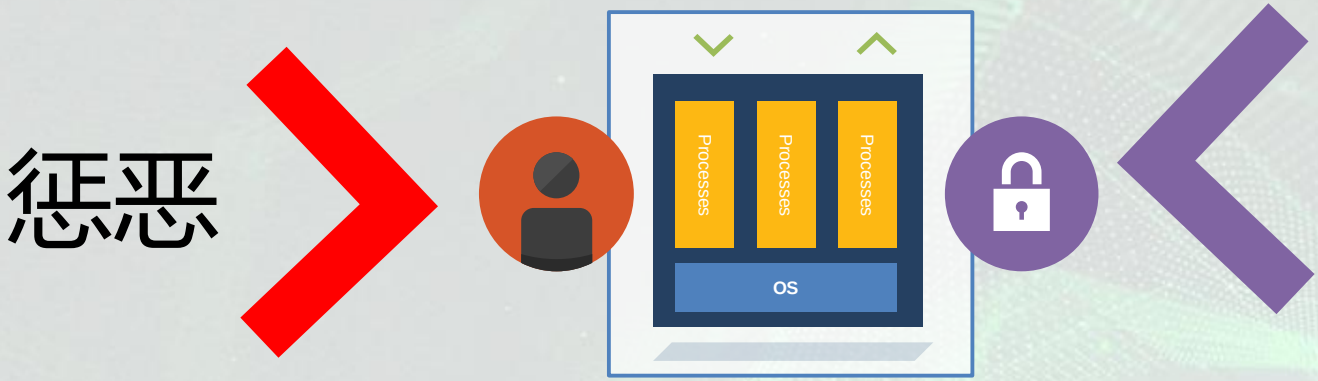
协作的力量

医 生

了解你的孩子可能面对的潜在疾病

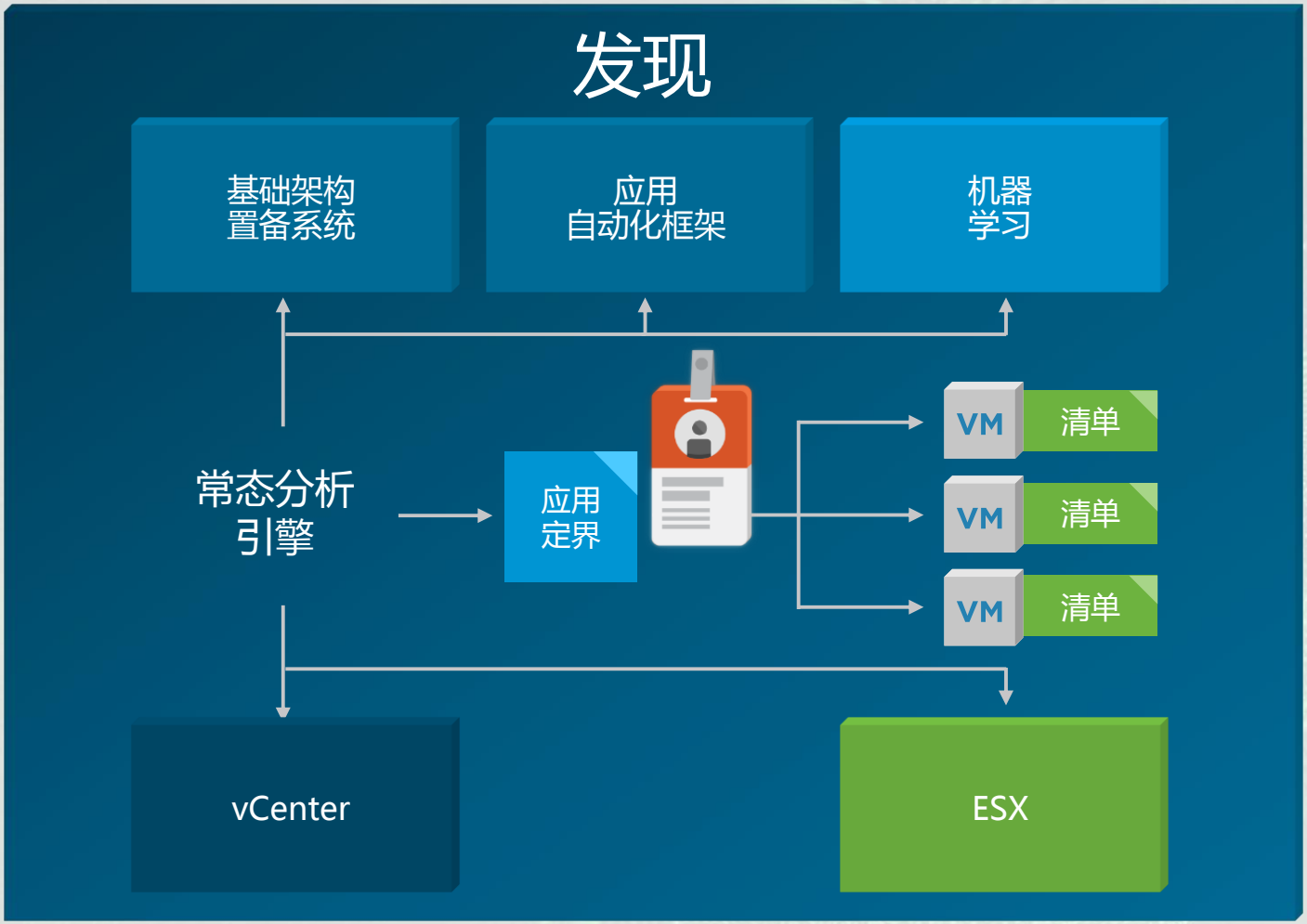
协作的力量

转变安全模型



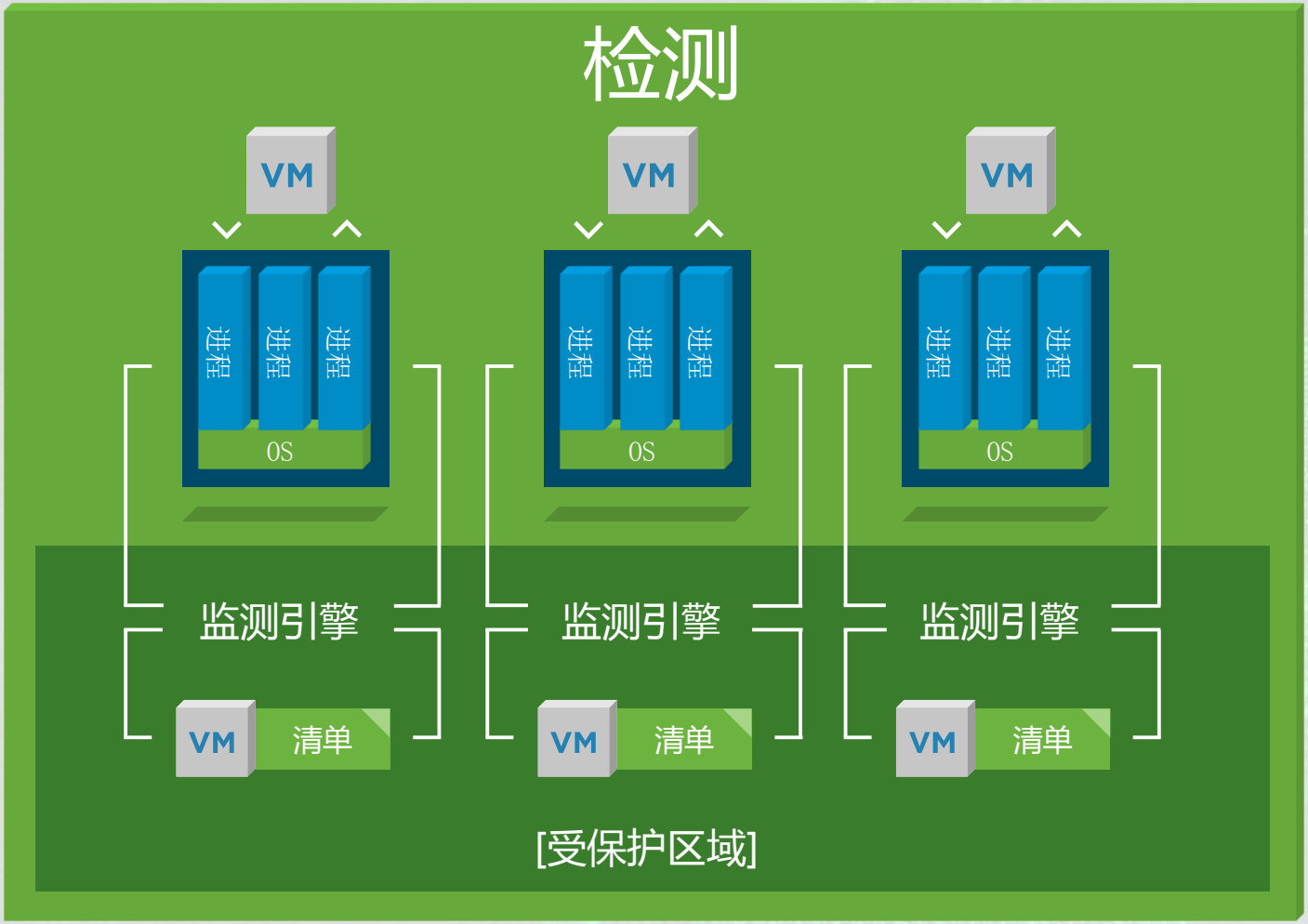
自动发现

自动发现应用并记录状态



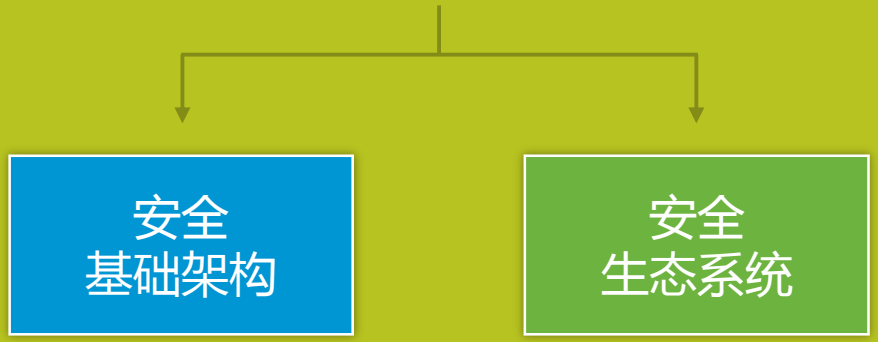
连续监测

实时监测针对应用和系统所做的改变



主动响应

事件响应的协作与自动化



利用vSphere，NSX和合伙伙伴的解决方案一起建立事件自动化响应流程，包括“快照”，“挂起”，“阻止/告警”，“隔离”，“网络阻断”，“服务注入”……

云模式下的协作与分工

安全架构与工程

安全运维中心

核查

应用的
编排和行为

就绪

应用
保护策略

监测

安全地
监测偏离

响应

触发
自动化响应

发现

检测

响应

热点案例分享

建设目标：通过虚拟桌面技术构建数据围栏，以保护开发部门的数字化资产。

解决方案：桌面虚拟化 + 微分段

方案价值：提升数据安全、网络安全(零信任安全)与主机安全(无代理终端安全)

勒索病毒紧急响应流程：

*① **添加1条防火墙规则(1分钟)**，禁止网络节点之间通过445端口通讯；*

*② **通过VDI母版快速更新(1小时)** 微软MS17-010补丁。*

总结：混合云环境下的安全体系架构

谢　谢


ISC
2017
5th
2017 中国互联网安全大会
China Internet Security Conference
万物皆变 人是安全的尺度
Of All Things Human Is The Measure