思科以应用为中心的基础设施 (ACI) 安全解决方案

优化和自动化当今的
动态数据中心的安全性

免责声明

本演示中介绍的许多产品和功能处于不同的开发阶段，将在可用时提供。

思科可自行决定更改此路线图，并且对本文档中列出的任何产品或功能的交付延期或无法交付，思科概不负责。

议题

- 正在推动数据中心转型的主要趋势
- 传统的安全方法不适用于现代数据中心
- 数据中心安全性必须朝着以应用为中心的方法发展
- 充分利用以应用为中心的基础设施安全解决方案
- 您是否已经为以应用为中心的安全解决方案做好准备？
- 简化、自动化、优化、扩展

当前动态

思科将为下一代数据中心和云应用开创**以应用为中心的基础设施**的新时代

思科将利用**以应用为中心的智能网络安全创新来发展自己的自适应安全设备产品组合**，从而优化、简化并自动实现跨物理和虚拟环境的安全保护

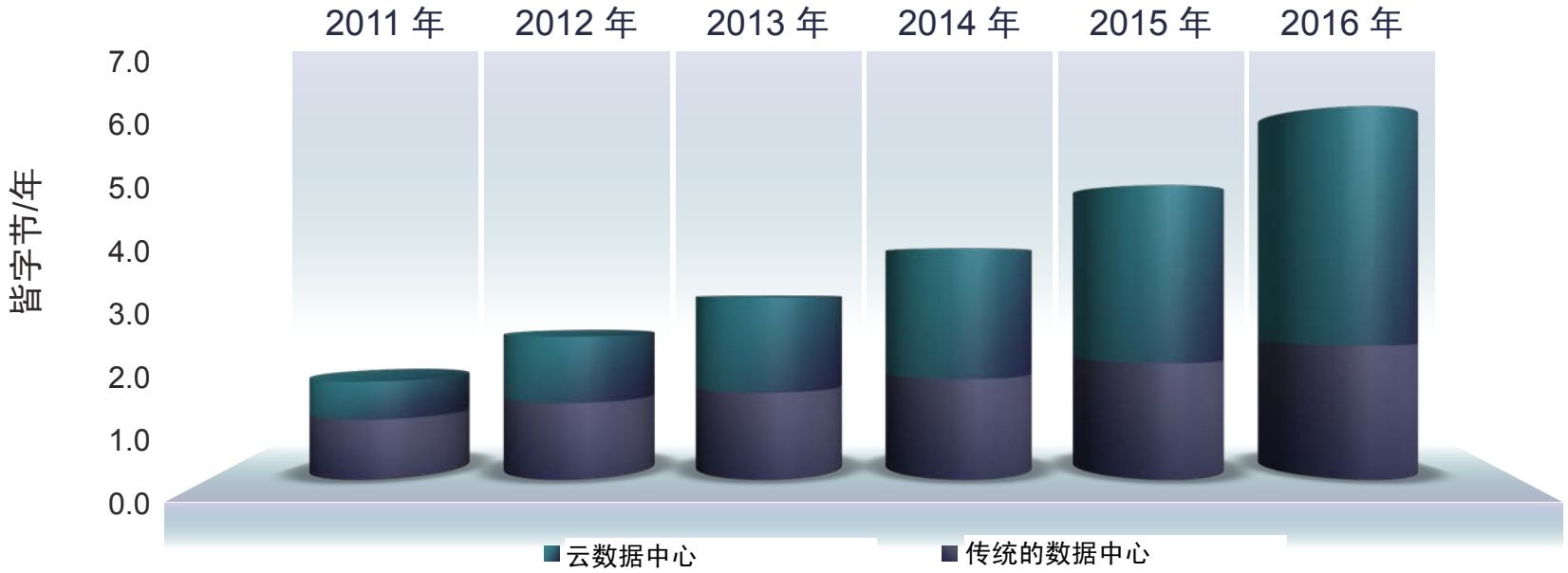
思科将推出**面向虚拟环境的自适应安全设备技术**

正在改变数据中心的主要趋势

全球数据中心流量：传统和云

到 2016 年，云流量将占数据中心流量的将近三分之二

2011–2016 年 CAGR（复合年均增长率）为 31%



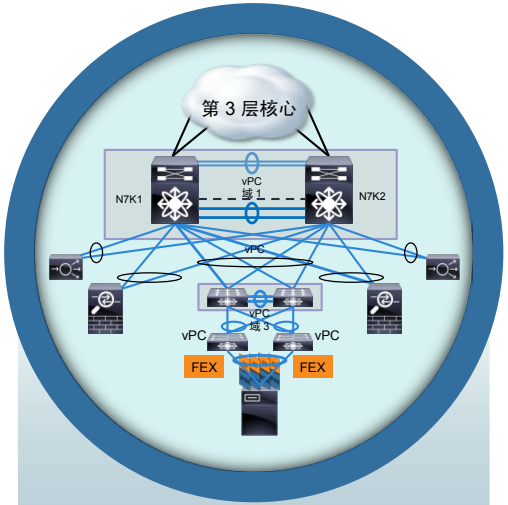
来源：2012 年思科® 全球云指数

按目标划分的全球数据中心流量

应用环境不断变化

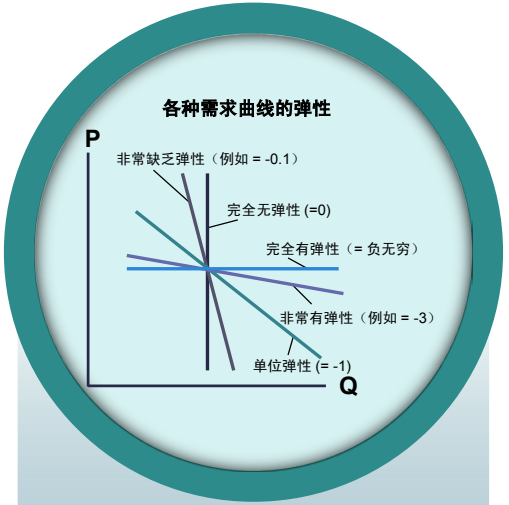
静态工作负载	移动工作负载
物理服务器	虚拟服务器
固定策略	动态策略实例化
IT 控制的应用	自带应用
长期通信流	短暂通信流

传统的安全方法不适合现代数据中心



在不灵活的“孤岛”
中插入的安全性

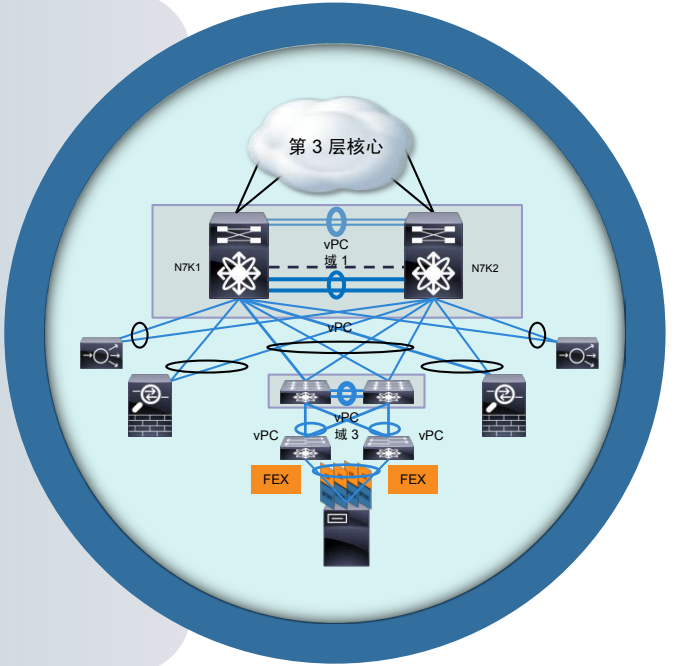
手动调配导致
复杂性增加



安全性无法实现
弹性扩展

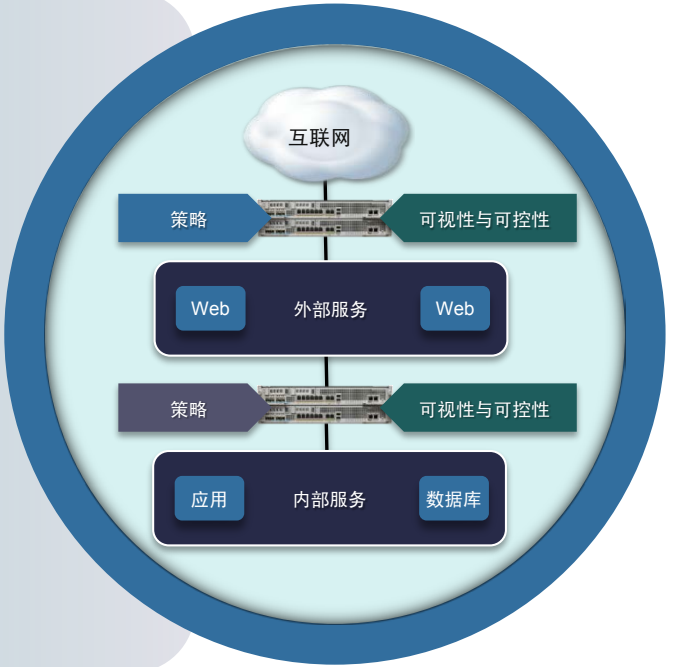
孤岛部署使安全性变得不灵活

- 以边界为中心的安全方法
- 进行服务插入必须对网络结构（例如 VLAN、子网等）十分了解，部署限定在网络中的固定位置
- 检测东-西流量既复杂又昂贵



传统的安全方法专注于边界

- 要求通过一个中央控制点路由流量，以便获得可控性和可视性
- 服务拼接是容易出错的手动流程
- 检测东-西流量既复杂又昂贵



手动的安全调配无法适应动态的工作负载

- 静态的策略调配无法轻松适应动态的工作负载
- 每台设备的防火墙规则数量呈爆炸性增长
- 多租户部署难以实施
- 容易出错的安全策略生命周期管理
- 多个管理域

手动的安全策略变更管理容易出错

应用
更改导致业务中断

80.6%
因与应用有关的规则更改而出现中断、安全漏洞或网络性能下降。

30.7% 应用中断
29.1% 网络中断
20.7% 性能下降

流程是
一个问题

60%
将手动流程、变更管理不佳和缺乏可视性确定为在管理安全设备时遇到的最大挑战。

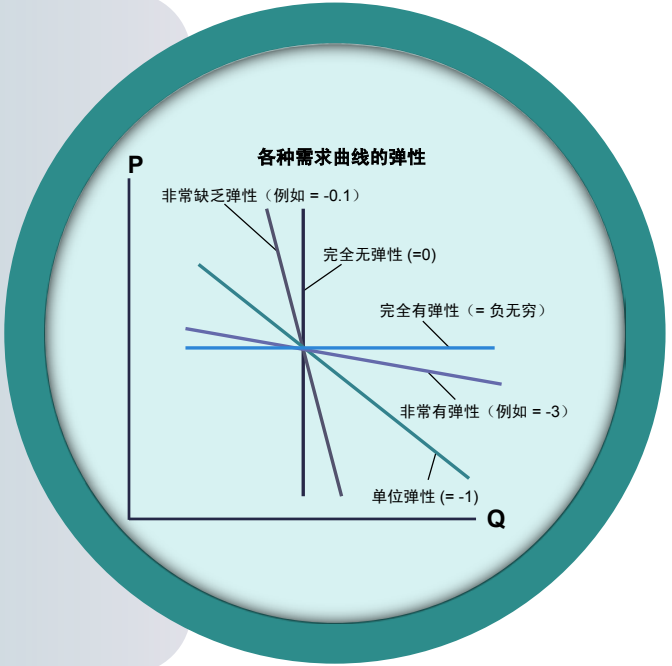
流程外的防火墙更改
增加了停止运行时间！

流程外！

流程外！
76.6%
因流程外的更改而遭受网络或应用中断

传统的安全方法无法有弹性地扩展

- 实施涵盖物理和虚拟工作负载的策略需要复杂的流量引导设计
- 超额调配以满足应用和安全服务级别协议 (SLA) 要求
- 安全资源使用效率低



传统的安全需求仍然存在

数据中心安全性必须与时俱进
采用以应用为中心的方法

容易且简单

- 应用作为安全性的推动因素
- 集中的控制点

快速！

- 可编程
- 自动化
- 能够按需横向扩展和纵向扩展

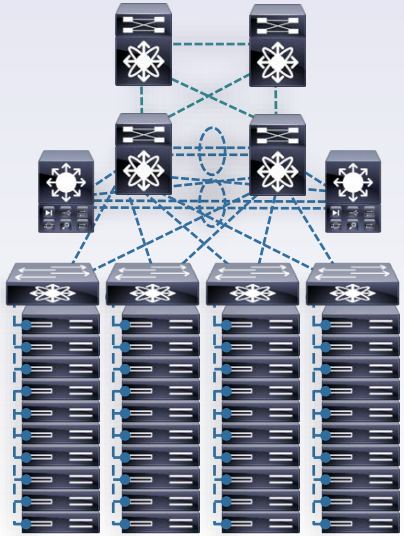
具成本效益和恢复能力

现代数据中心的安全要求

动态的工作负载	▪ 动态地实例化和移除应用工作负载
异类	▪ 涵盖物理和虚拟基础设施的部署
分布式部署	▪ 按需横向扩展/纵向扩展调配
独立于基础设施	▪ 对底层网络基础设施透明
感知云	▪ 旨在无缝迁移到公共云和私有云

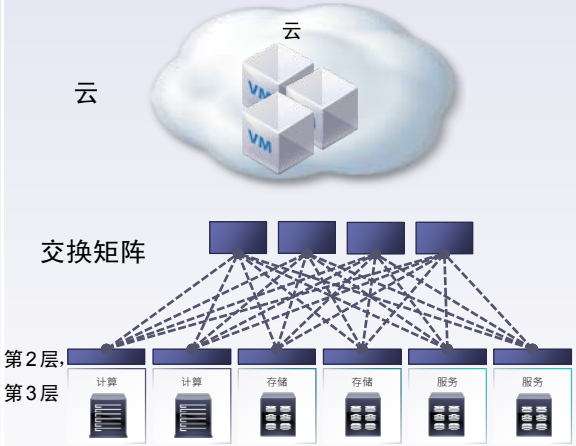
安全性必须与数据中心一起发展

分布式



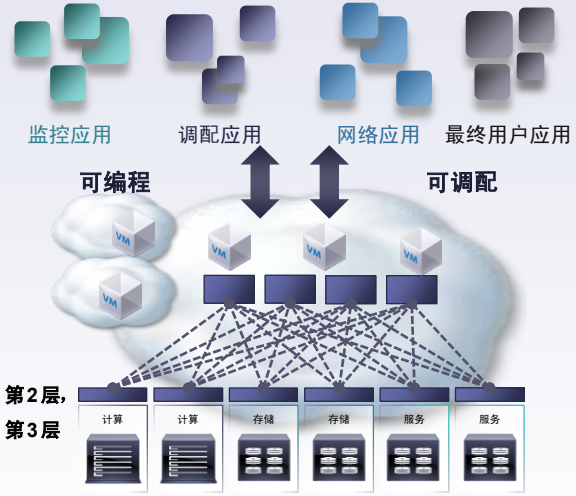
- 手动调配
- 有限扩展
- 机架范围的虚拟机 (VM) 移动性

基于交换矩阵



- 基于策略的调配
- 扩展物理、虚拟和云
- 数据中心范围/跨数据中心的 VM 移动性

应用驱动



集成的交换矩阵和云；充满云的世界

- 以服务为中心的调配
- 灵活 – 随时随地
- 跨越云的 VM 移动性

以应用为中心的安全

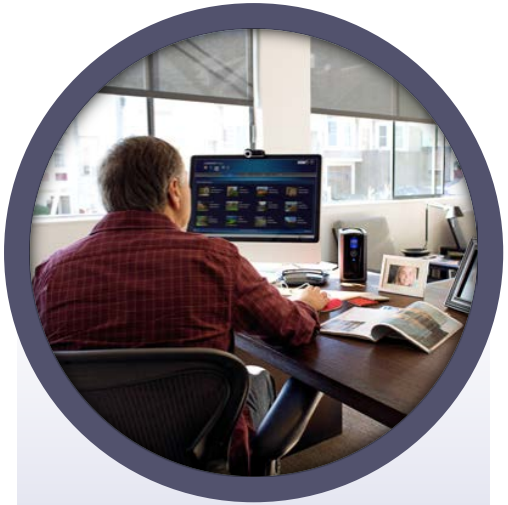
- 安全即服务不再具有策略的控制权，而是感知威胁
- 服务拼接很简单，并且由网络动态地管理
- 东-西流量检测很简单，并且可以为特定的应用快速插入服务

以应用为中心的安全性应当具有开放性和灵活性

充分利用以应用为中心的基础设施 (ACI) 安全解决方案

以应用为中心的基础设施安全解决方案简介

将安全平台透明地集成到
智能网络交换矩阵



集中式策略管理
和自动化

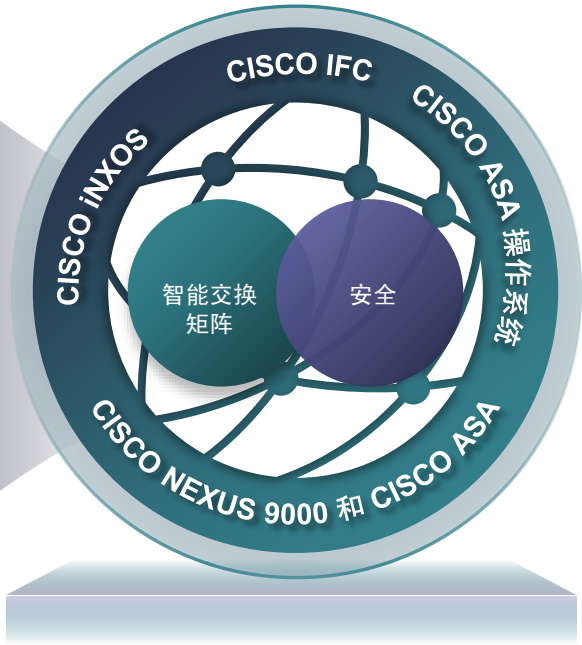
涵盖虚拟化和非虚拟化
环境的弹性可扩展性

将思科安全平台集成到智能网络

扩展
- 虚拟封装支持
- 支持具有状态同步功能的 N 路集群
- 用于按需扩展的安全资源池

融合
- 应用之间的 ASA 的无缝服务拼接
- 集中式管理和自动化
- “一次布线”理念

智能
- 一致的安全策略实施（物理和虚拟）
- 主动监控和全面诊断以缓解威胁

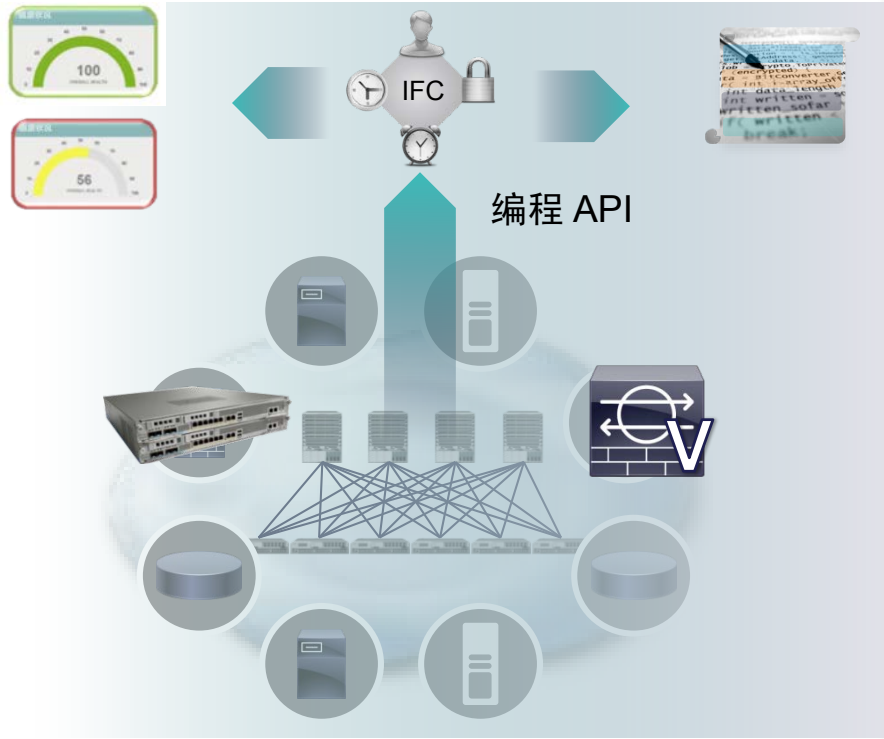


集中式策略管理和自动化

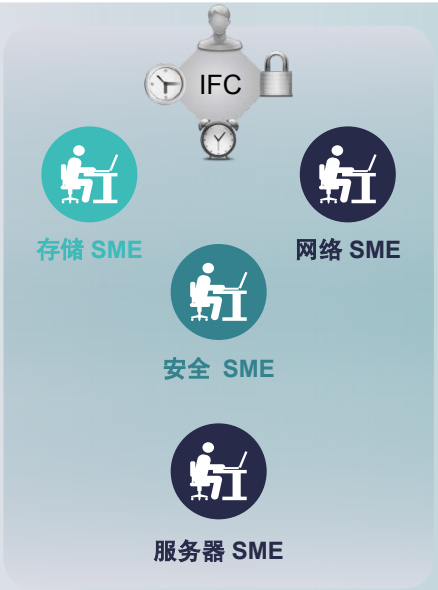
智能交换矩阵控制器

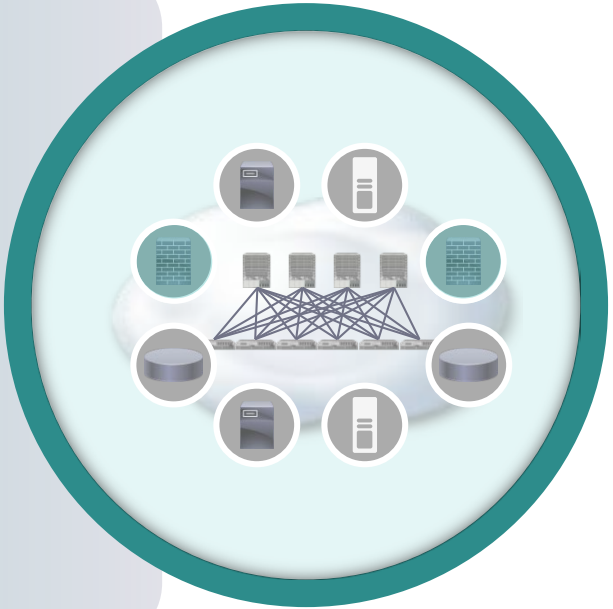
集中式策略管理和自动化

- 南向 RESTful API
- 基于角色的访问控制 (RBAC)
- 安全策略模板创建
- 遥感勘测功能



智能交换矩阵：自动化
集成、以业务为中心的安全应用策略





1. 主题专家定义应用之间的策略合同
2. 合同在端点之间提供保证，生成应用模板
3. 应用模板用于创建应用网络配置文件
4. 将应用网络配置文件与交换矩阵关联会自动配置应用资源

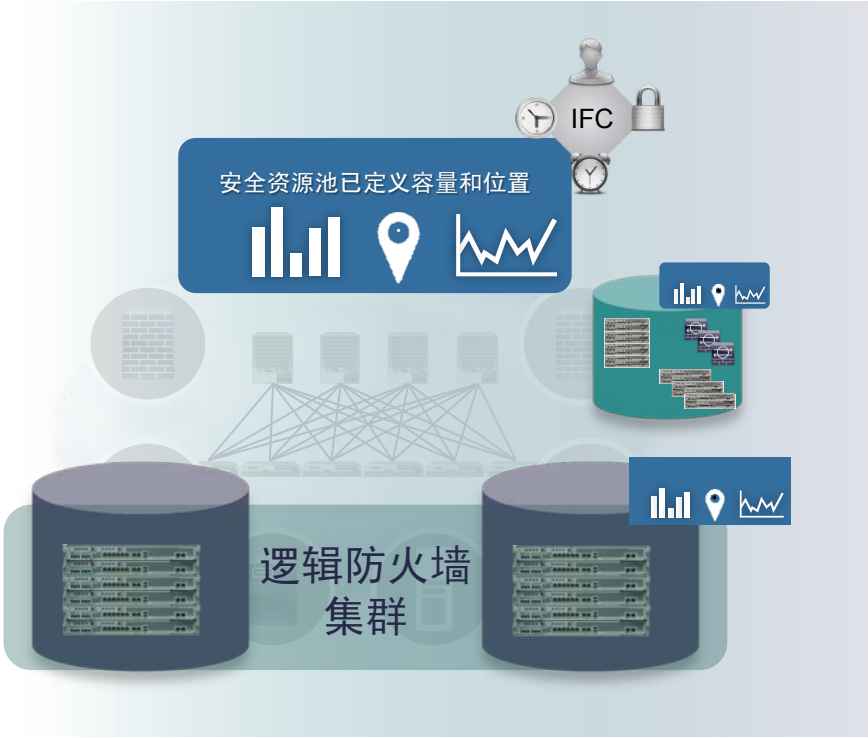
弹性扩展

安全资源池

按需横向扩展安全性

- N 路非状态负载分配
- 具有状态同步功能的 16 路负载分配*
- 适用于不同类型的虚拟基础设施
- 涵盖物理和虚拟设备的池
- 位置感知型智能流量引导，便于实施安全策略

*仅限物理 ASA 集群



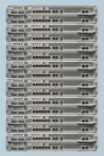
思科自适应安全设备

虚拟

Vmware 威睿	Red Hat Linux
Xen	Windows

- 虚拟机监控程序支持
- 与虚拟交换机无关

设备



- 具有状态同步功能的 16 路负载分配
- 扩展至最高 640 Gbps 的吞吐量

常见的 64 位操作系统和功能

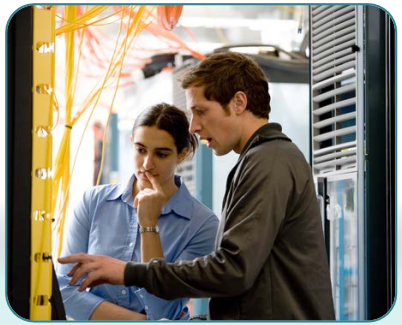
智能交换矩阵感知型
南向 RESTful API 支持；重叠协议支持 (VXLAN)

思科自适应安全设备

以应用为中心的智能安全产品组合

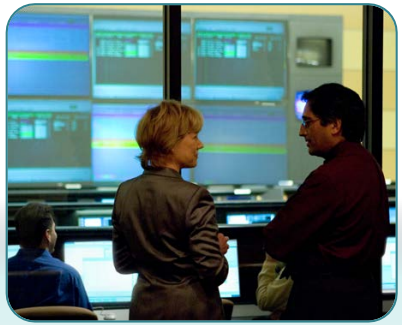
专为实现灵活性、可扩展性、可编程性和应用感知而设计

优化安全性
为网络构建智能功能



确定潜在威胁
并更改策略

预测



通过在全球范围内拦截
来控制威胁

修复

向智能交换矩阵
告知威胁

传达

发展为以应用为中心的安全性

- 统一安全、网络和计算资源
- 提供可编程、自动化的安全性
- 提高对物理、虚拟和云环境的可视性和洞察力
- 采用按需横向扩展的安全基础设施优化资源
- 使安全性与现代的动态工作负载和流量模式保持一致
- 在数据中心以及公共云和私有云内部和之间实现无处不在的安全性

您是否已经为以应用为中心的安全解决方案做好准备？

思科是您可以信赖的安全合作伙伴

- 与跨职能部门的利益主体建立重要关系
- 衡量并审视安全策略的有效性
- 将以应用为中心的有效安全行为灌输到组织文化中，并促进业务创新
- 利用 ACI 安全解决方案，采用新的思维方式

思科以应用为中心的基础设施安全解决方案
简化、自动化、优化、扩展

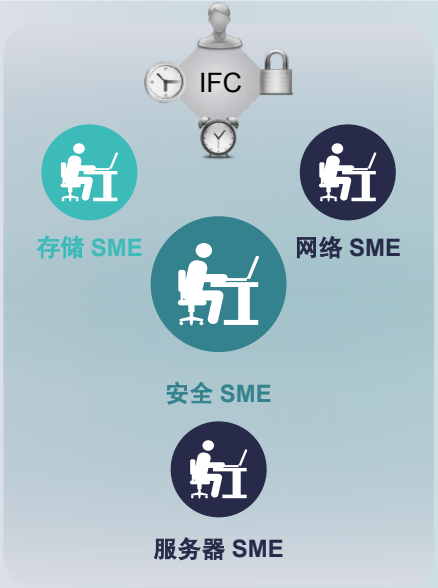
简单性	▪ 使用统一的安全、网络和计算基础设施简化和优化安全性
灵活性	▪ 通过自动化、可编程的安全性获得新的业务灵活性和洞察力
可扩展性	▪ 通过按需横向扩展的基础设施降低运营成本和资本成本
安全	▪ 借助应用感知型安全框架，在数据中心内部和之间实现更加无处不在的安全性

其他技术信息

论点

1. 集中式安全策略生命周期管理
2. 针对工作负载移动性推出的弹性安全服务
3. 高度安全的多租户
4. 针对跨越云的 VM 移动性推出的可扩展安全性

安全策略生命周期管理
集成的操作简便性



INET EPG　INET EPG　INET EPG

可满足所有 IT 监管需求的自动化安全策略生命周期管理

在任何给定的时间，有效的安全策略都位于设备上

完全避免设备上的策略规则呈爆炸式增长

1 安全主题专家定义应用安全策略合同

2 策略合同应用于应用网络配置文件

3 在 EPG 之间实施应用网络配置文件

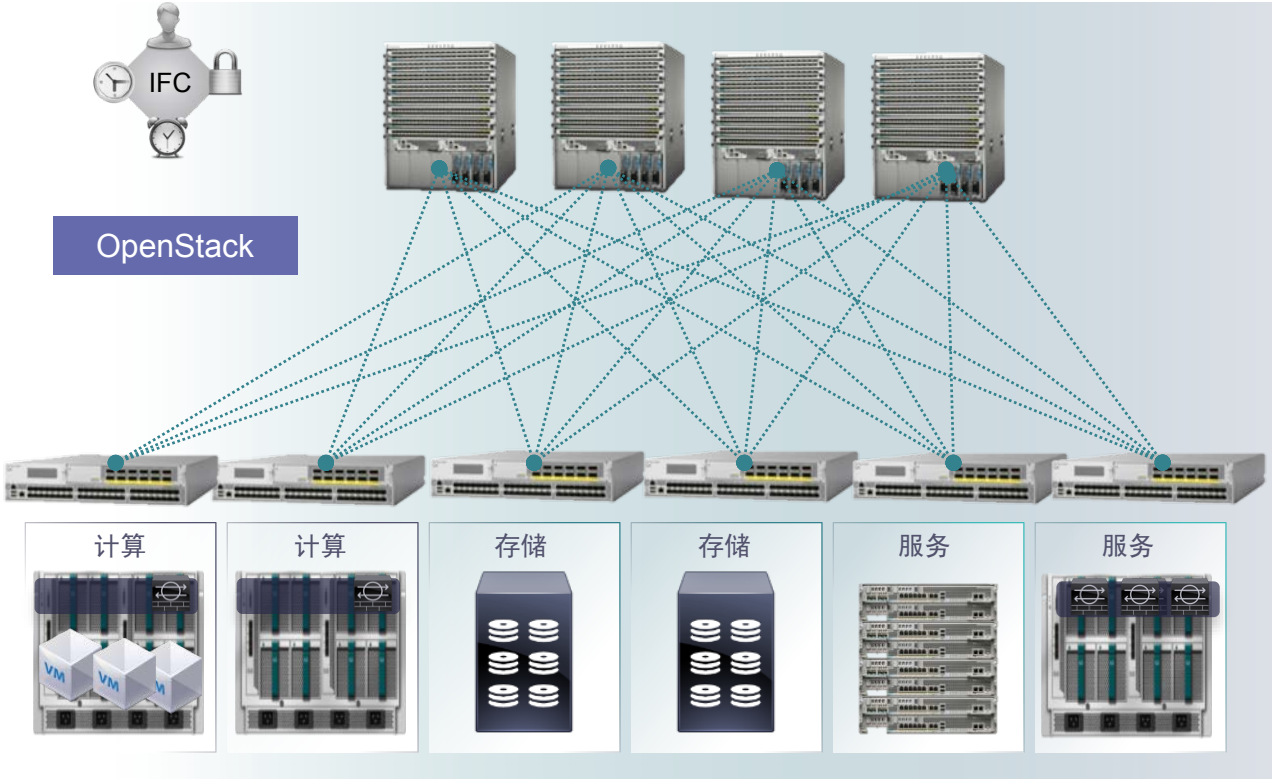
4 安全策略随着 EPG 停用而自动停用

安全服务的弹性调配

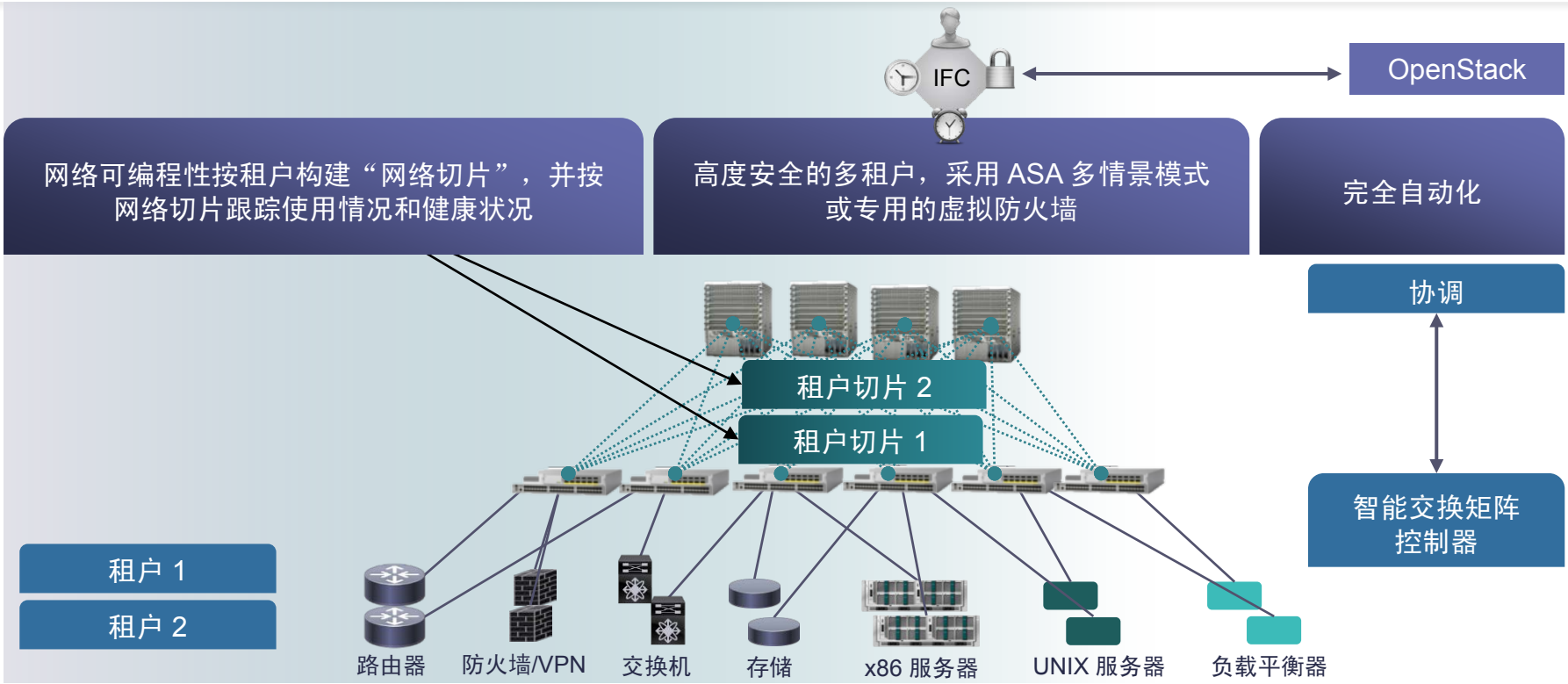
使用弹性扩展功能一致地实施策略

- 应用工作负载移至性能更高的主机
- IFC 与协调工具结合使用，调配更多的虚拟 ASA 防火墙
- 复制安全策略以便一致地实施

*仅限物理 ASA 集群

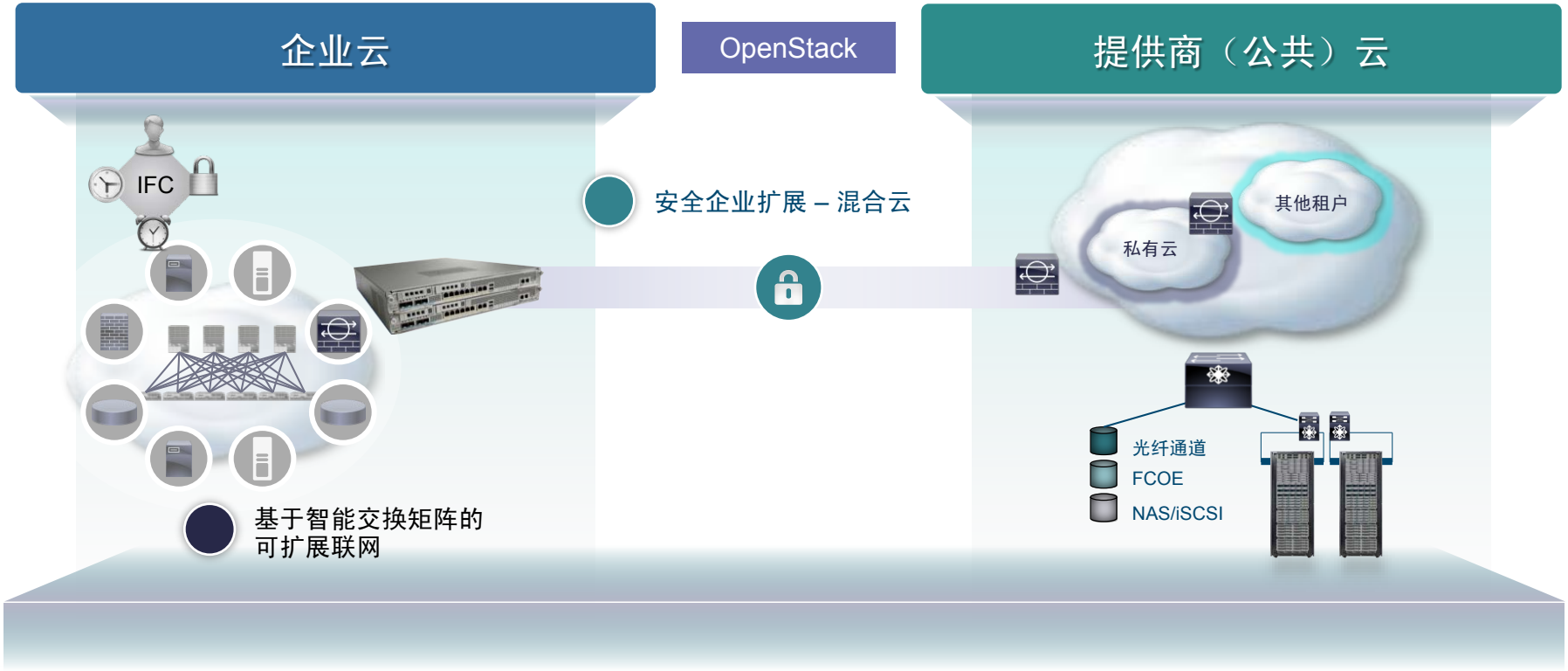


高度安全的多租户



使用智能网络扩展和延伸私有云

1 2 3 4



Cisco ACI 安全解决方案的论点支持因素

基础设施服务

协调

管理/监控

API

智能交换矩阵控制器

SNMP NETFLOW RESTful API CLI SNMP NETFLOW

ASA 操作系统（64 位内核）

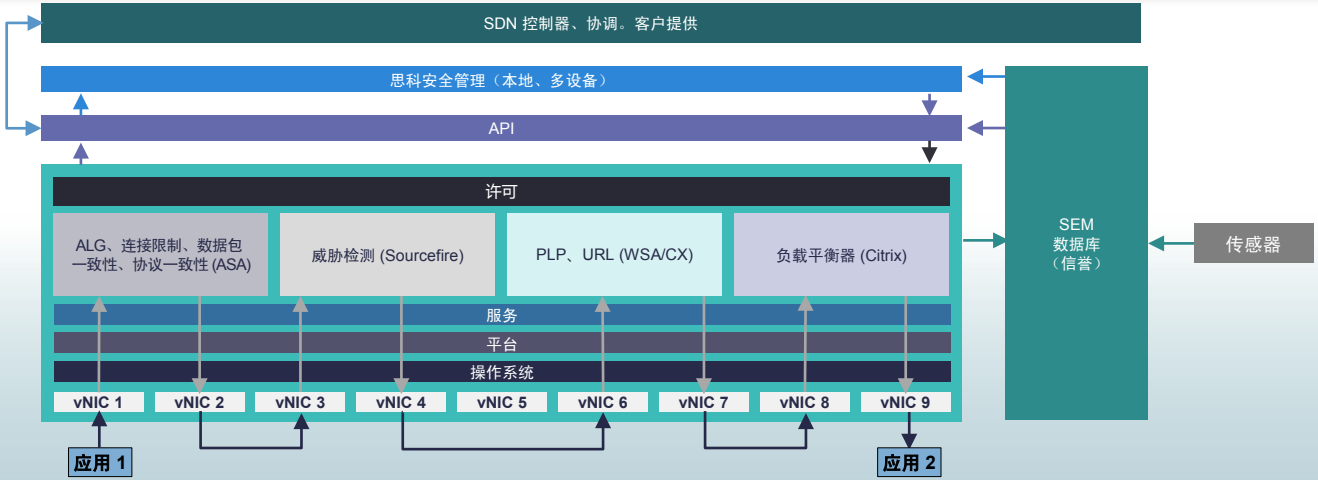
虚拟安全设备

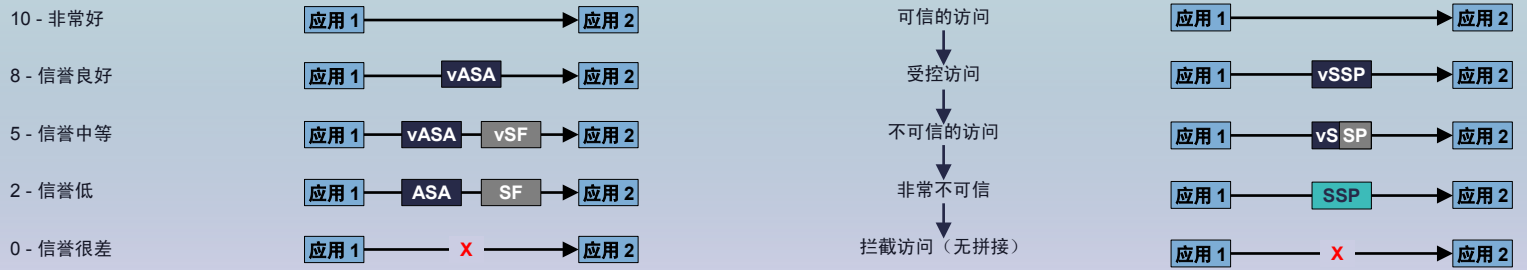
实体设备

以应用为中心的安全智能

交换矩阵的威胁防御

下一代解决方案（智能 SDN）





谢谢各位。