安全数据中心

发言人姓名
发言人职务

日期

本演示的内容要点

- 要应对各种各样的威胁，必须采用涵盖整个攻击过程的端到端解决方案
- 思科® 安全数据中心提供轻松的自动化、最佳的性能和切实可行的保护
- 以三个层面为基础：1) 基于角色的管理；2) 简化且可扩展的安全性以及 3) 融合网络基础设施
- 通过 Cisco Secure Enclaves Architecture 部署数据和应用的服务级别层
- 通过策略矩阵提供对数据中心资产的简化授权访问
- 使用安全组标记 (SGT) 将安全策略附加至工作负载
- 基于思科认可设计 – 可以轻松部署的经过验证和测试的概念

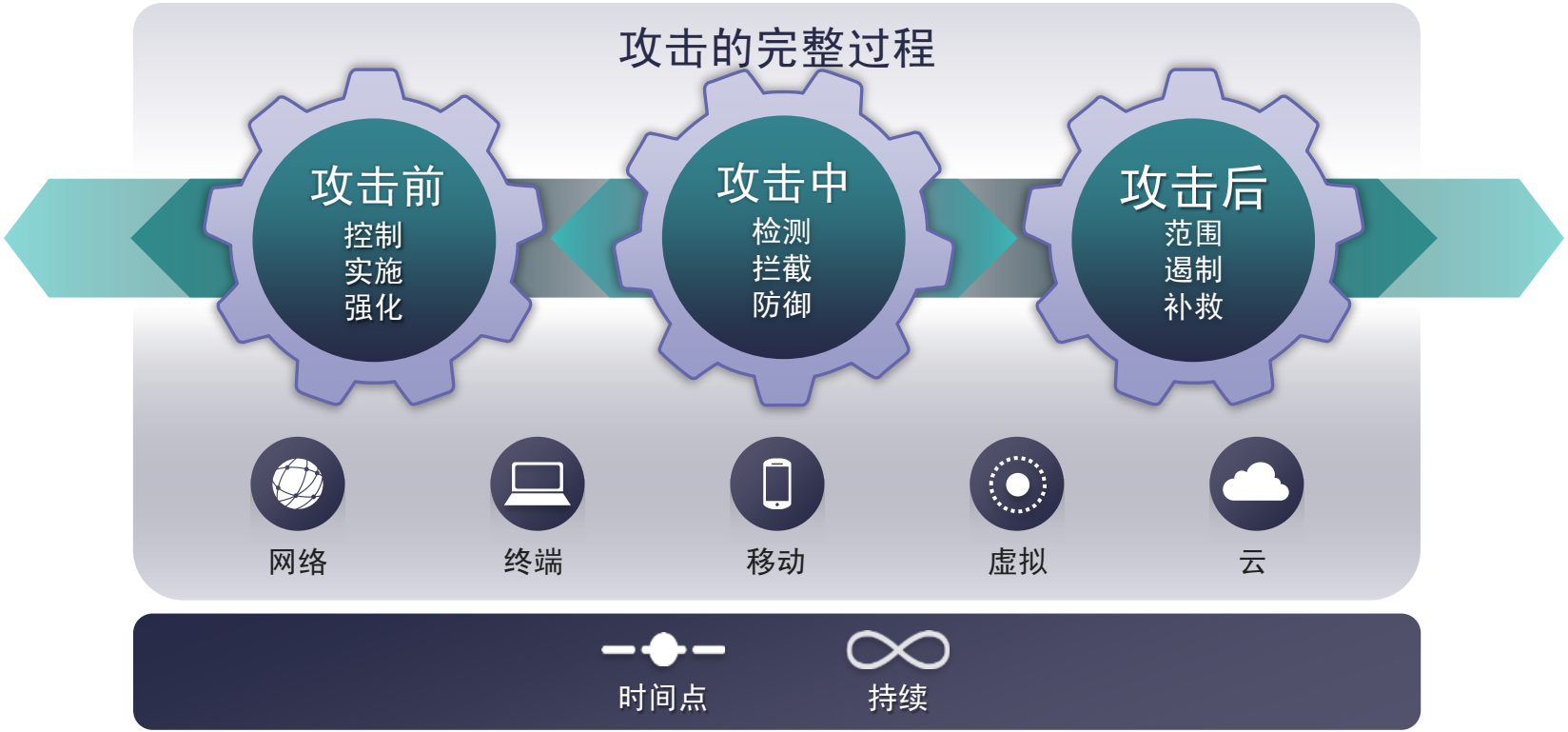
安全问题

不断变化的
业务模式

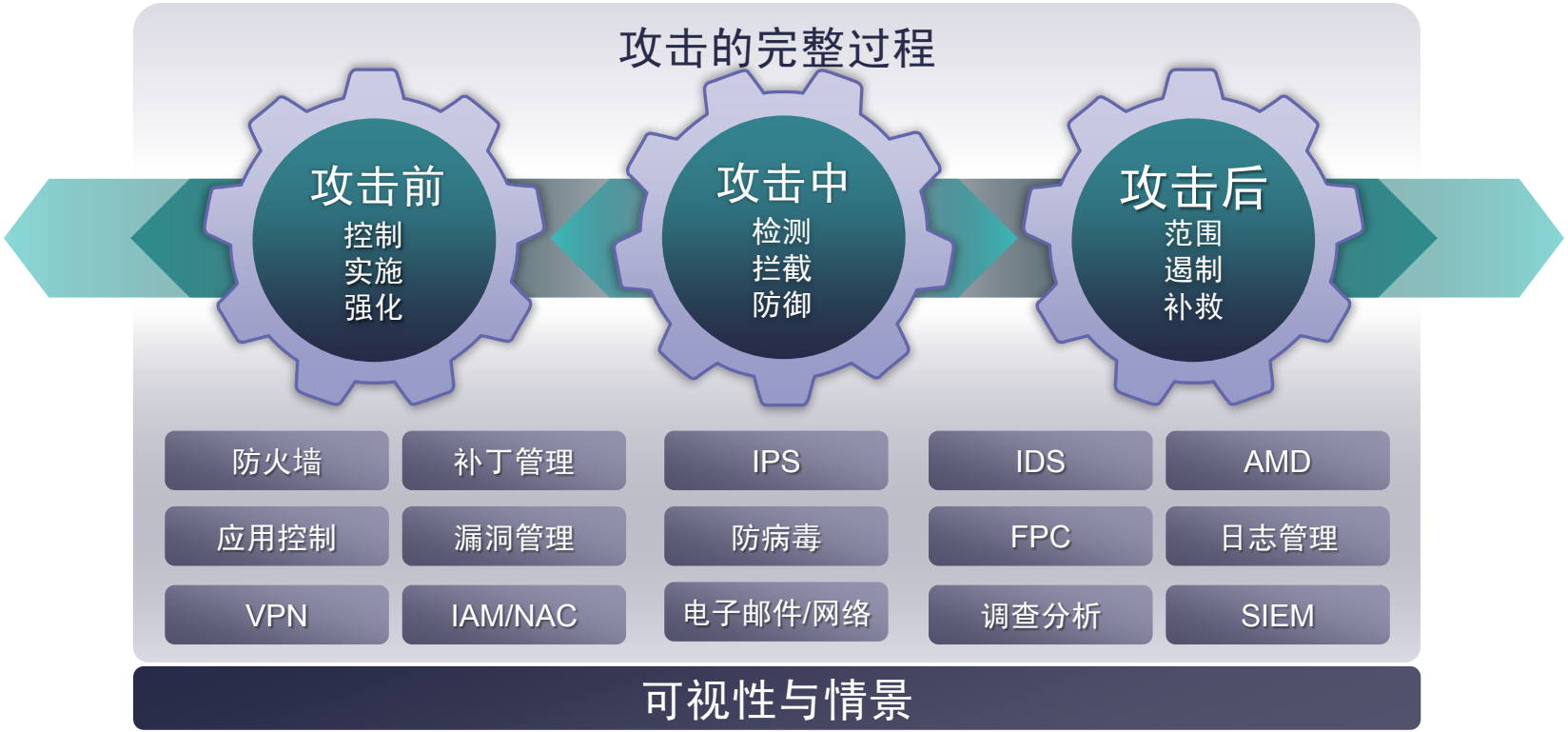
瞬息万变的
威胁形势

复杂性
与凌乱性

新安全模式



涵盖整个攻击全程



思科安全数据中心的设计支柱

轻松的自动化

- 将高度安全的新服务的部署时间从几周缩短至几小时
- 将策略管理工作减少 80%
- 将合适的工具提供给合适的团队

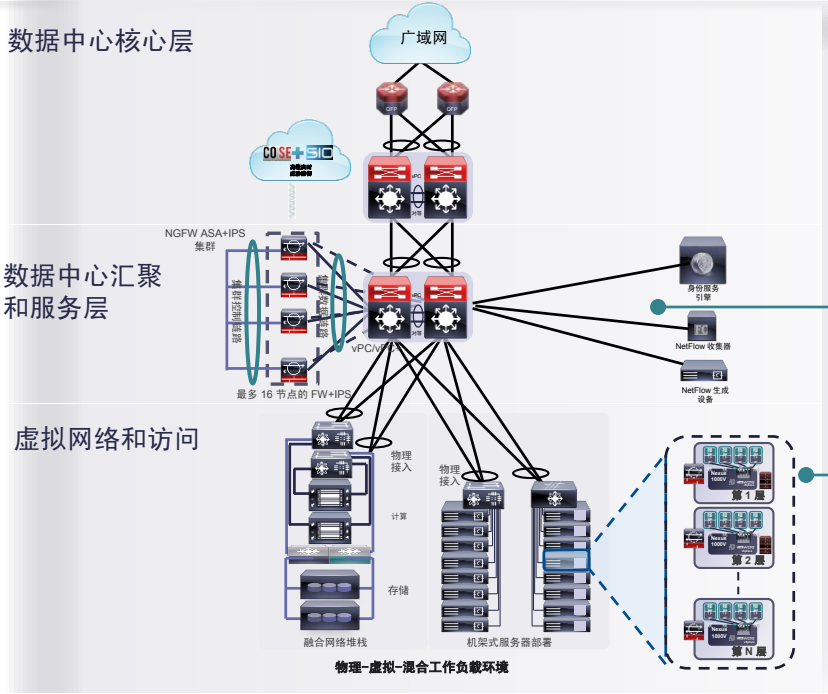
最佳的性能

- 防火墙的性能比竞争对手高 8 倍
- 增强的可用性和恢复能力
- 使安全性能与网络性能相匹配
- 不对称的流量

切实可行的保护

- 南-北保护
- 东-西保护
- 基于签名的保护
- 基于信誉的保护
- 无签名保护

适用于企业的安全数据中心
思科® 认可设计能够降低风险并加快部署速度



基于角色的管理

安全性、思科认可设计

简化且可扩展的安全性

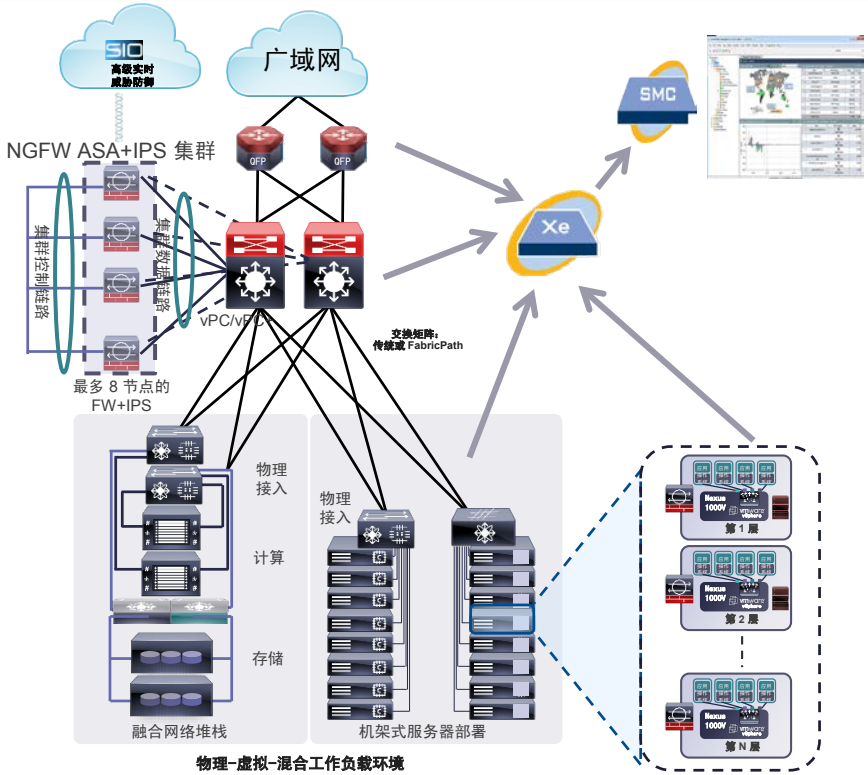
思科自适应安全设备 (ASA) 集群、TrustSec®、用户身份、零日威胁缓解

融合网络基础设施

Vblock、Flexpod、虚拟系统规格 (VSPEX)、历史数据服务器 (HDS) 参考架构

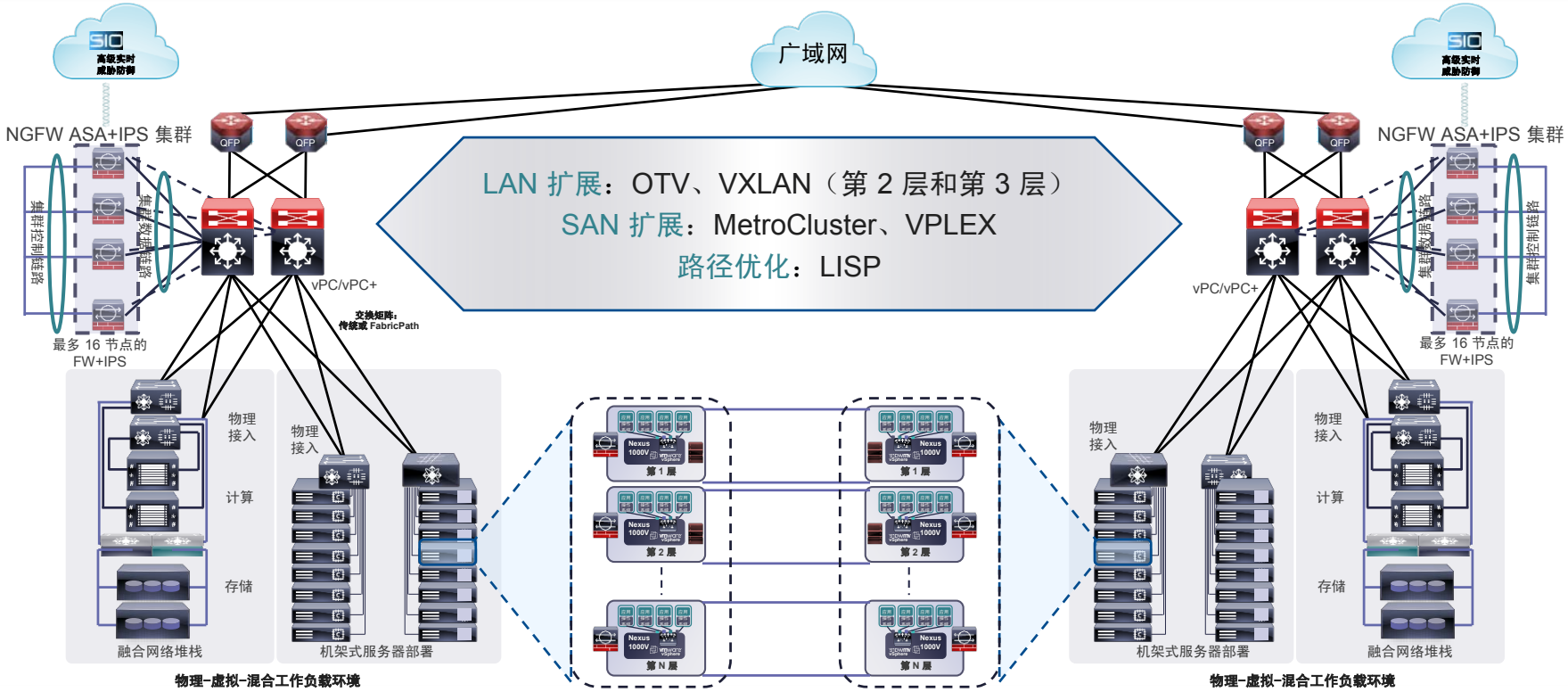
经验证的 兼容性 | 可扩展性 | 可靠性

适用于企业的思科安全数据中心
扩展数据中心



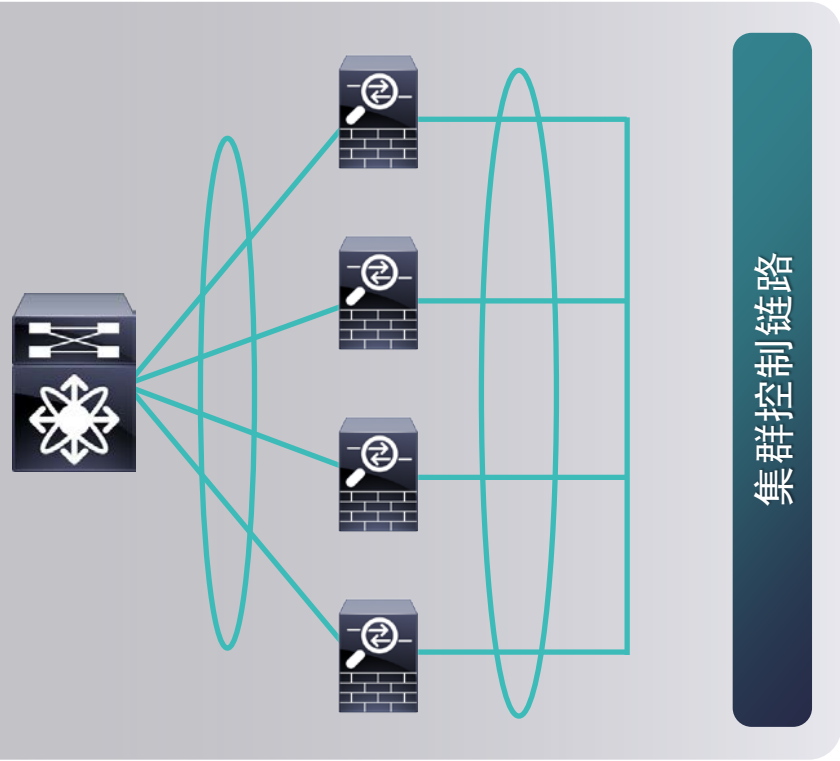
自动化	性能	保护
安全操作： 思科® 安全管理器	**扩展：** ASA+IPS 集群 高达 640 Gbps 的防火墙 高达 160 Gbps 的 IPS	**南-北：** ASA+IPS NGFW **东-西：** 虚拟安全网关
服务器操作： Cisco UCS® Director	**可靠的数据流：** 不对称的流量	**基于签名：** IPS+SIO **基于信誉：** IPS+SIO
网络操作： 数据中心网络管理器	**交换矩阵集成：** vPC、LACP、cLACP	**内部部署的无签名保护：** Lancope Stealthwatch **基于云的无签名保护：**SIO
自动化： Prime 网络服务控制器	**第 2 层可扩展性：** FabricPath、VXLAN、OTV	**内部行为分析：** Lancope Stealthwatch **基于云的行为分析：**SIO
策略汇聚： 安全组标记	**虚拟化层：** vPATH 服务链	**应用分段：** 安全组标记

思科安全数据中心
跨多个站点扩展 – 计划

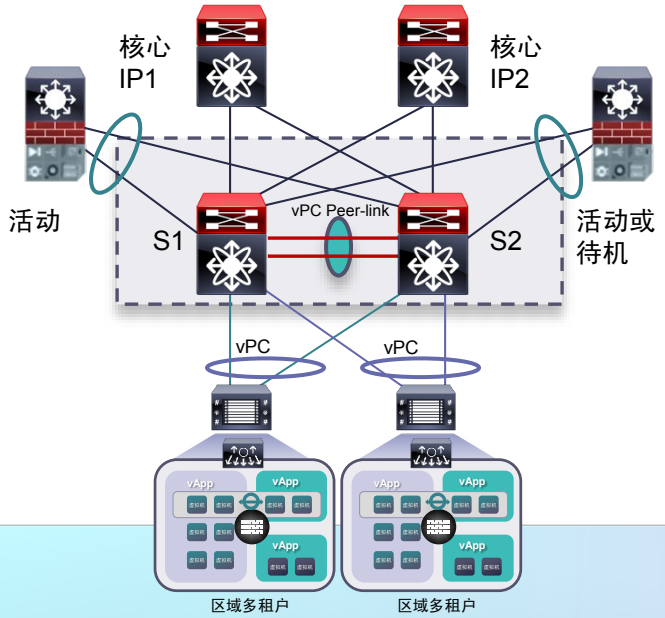


数据中心性能
南-北保护和数据中心边缘

- 扩展以满足业务需求
  - 最多 8 台 ASA 5585 设备的集群
- 高达 80 Gbps 的 IPS 吞吐量扩展
- 支持非对称流
- 连接流量具有冗余
- 群集内高可用性



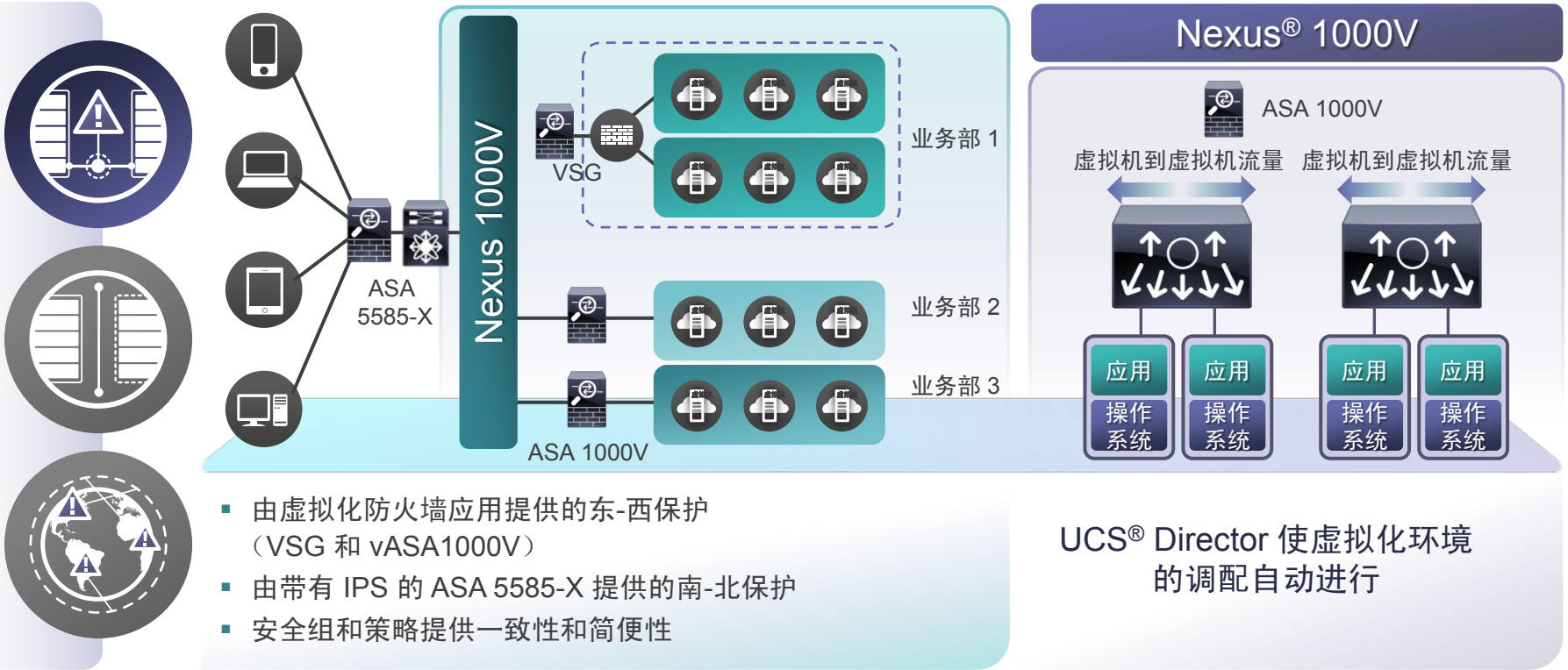
优化网络性能



- 更高的可用性
  - 通过 vPC 的所有可用流量链路的正常运行时间
- 更高的网络恢复能力
  - 不对称的流量帮助确保避免网络异常或流量损失
- 强大的可扩展性
  - 对通过 Cisco® FabricPath 的东-西流量无带宽限制

虚拟端口通道 (vPC) 和 FabricPath 创新提升网络性能

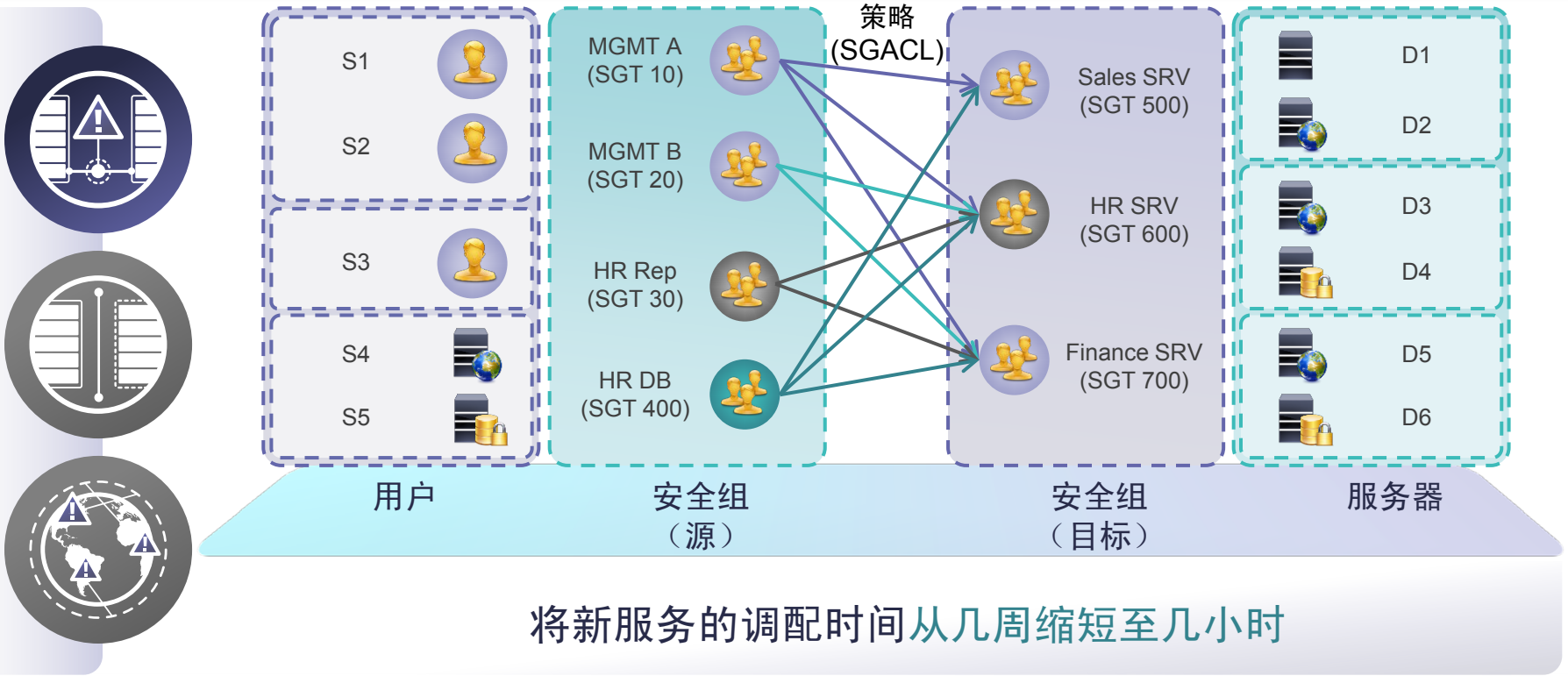
轻松调配



- 由虚拟化防火墙应用提供的东-西保护（VSG 和 vASA1000V）
- 由带有 IPS 的 ASA 5585-X 提供的南-北保护
- 安全组和策略提供一致性和简便性

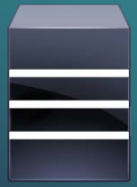
UCS® Director 使虚拟化环境的调配自动进行

将用户角色映射到数据中心资产角色



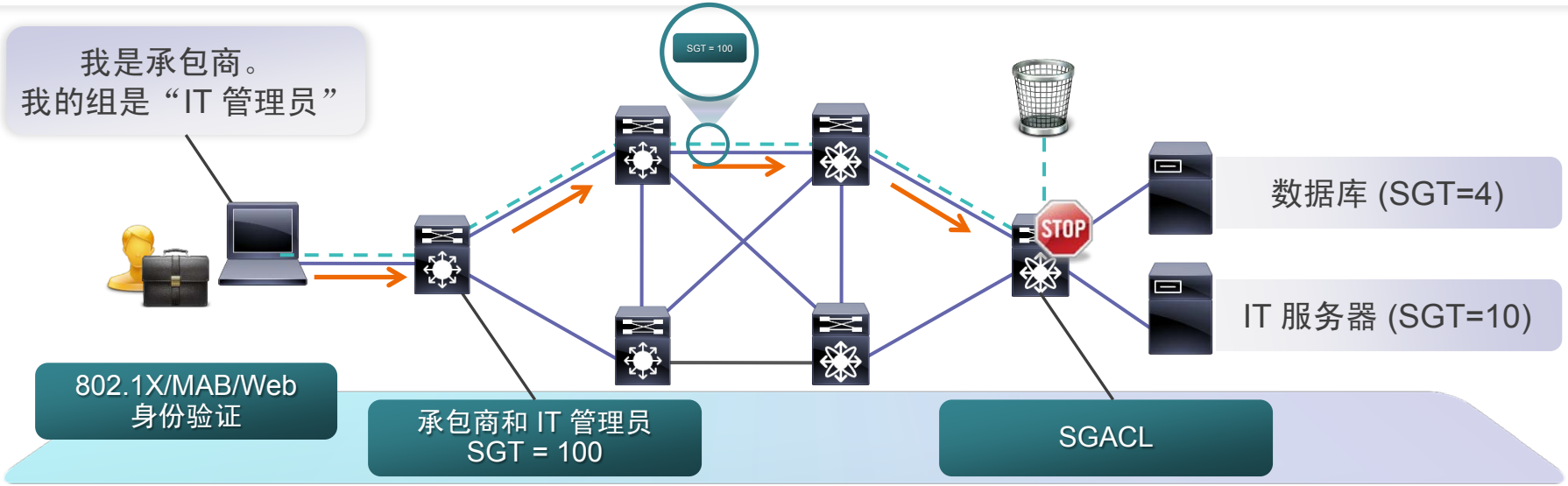
将新服务的调配时间从几周缩短至几小时

安全组访问控制列表 (SCAGL) 策略矩阵

目标 SGT / 源 SGT	 人力资源 (SGT 10)	 工程 (SGT 20)	 网络服务器 (SGT 40)	 邮件服务器 (SGT 50)
	Web	无访问	Web	Web 文件共享

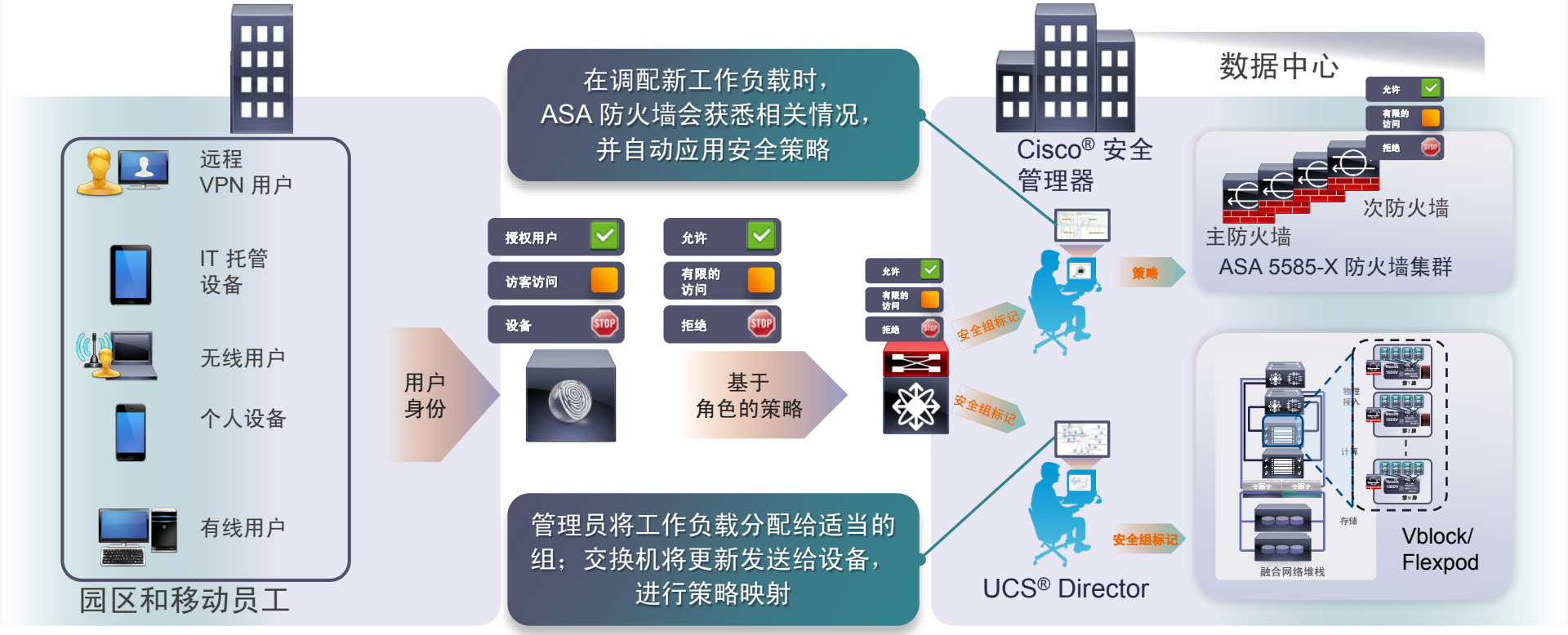
采用 Cisco TrustSec 的安全交换矩阵

支持 SGT 的设备



- 基于安全组的访问控制让客户可以：
  - 在接入层保留现有的逻辑设计
  - 更改或应用策略以满足现今的业务需求
  - 从一台集中管理服务器分发策略

简化整个企业的安全
端到端的 Cisco TrustSec（简化视图）



切实可行的保护

思科® 安全智能运营中心 (SIO)

- 来自超过 75 TB 数据分析的实时威胁源、超过 5500 个 IPS 签名
- 基于信誉的保护、基于身份和情景的策略、最新的加密算法

- 在威胁导致服务中断之前拦截它们
- 形成信任链 – 从用户到应用
- 提供实时签名和信誉更新
- 未来基于云的威胁防御

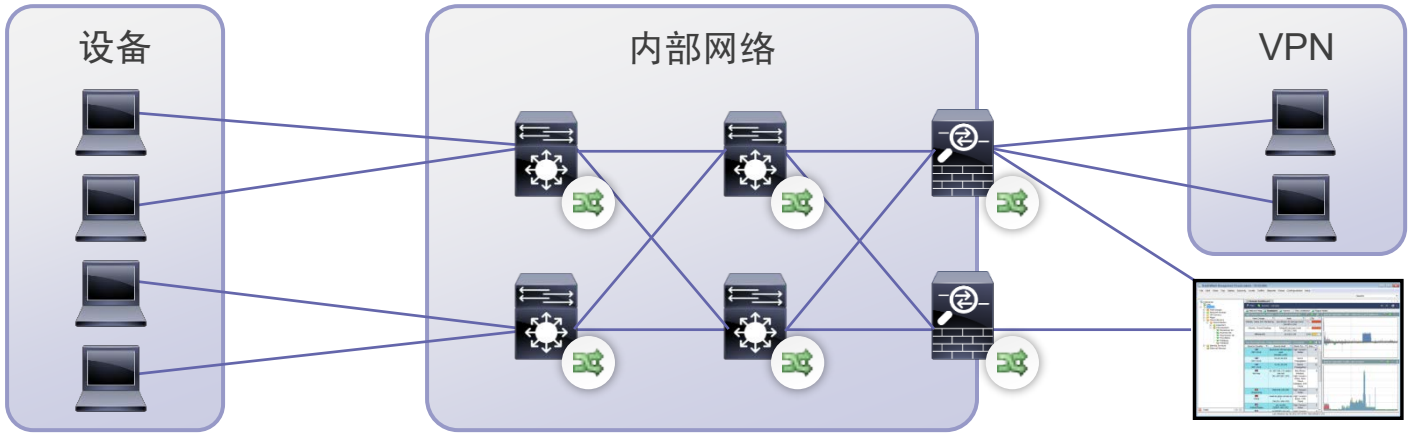
实现稳健、持续的服务交付

无签名保护

支持 NetFlow

人员　内容　地点　时间　方式

可视性、情境和可控性



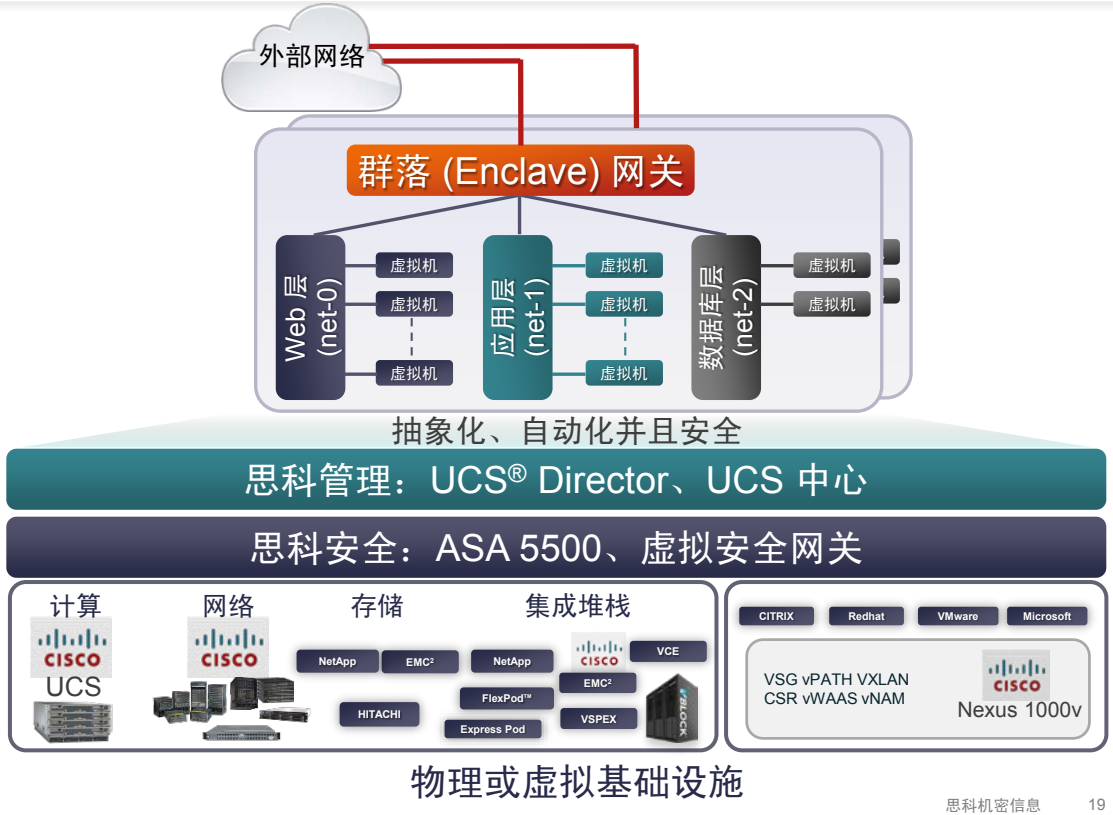
使用 NetFlow 数据将可视性扩展至接入层

使用身份和应用丰富流数据以创建情景

统一到单个视点以便调查和报告

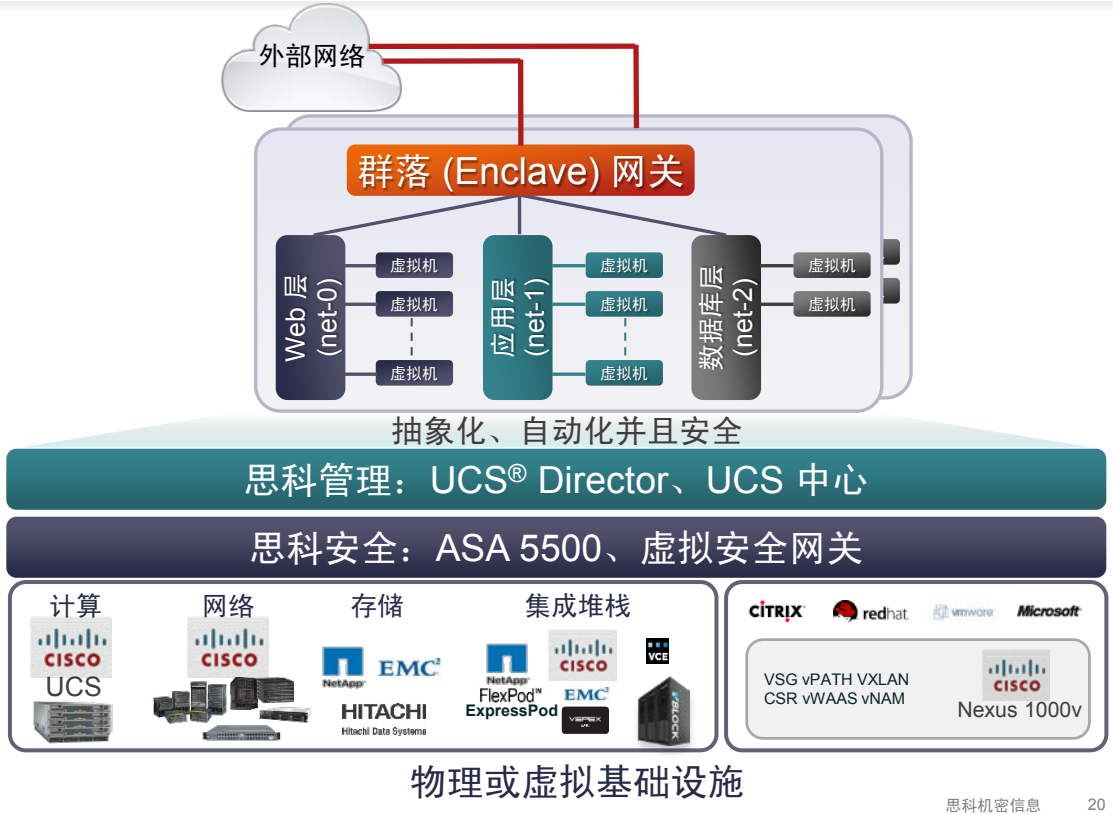
Secure Enclaves Architecture
自动化、异类、融合的基础设施

- 一种思科® 框架，适用于通过云进行高度安全、轻松的应用部署
- 将安全多租户 (SMT) 提升到新的水平
- 对于第 1 阶段：
  - 专注于通过自动化轻松进行部署
  - 超越 SMT 提高安全性
- 未来阶段：
  - 通过新的特性和功能不断改善框架
  - 通过异类云改善应用部署



Secure Enclaves Architecture
自动化、异类、融合的基础设施

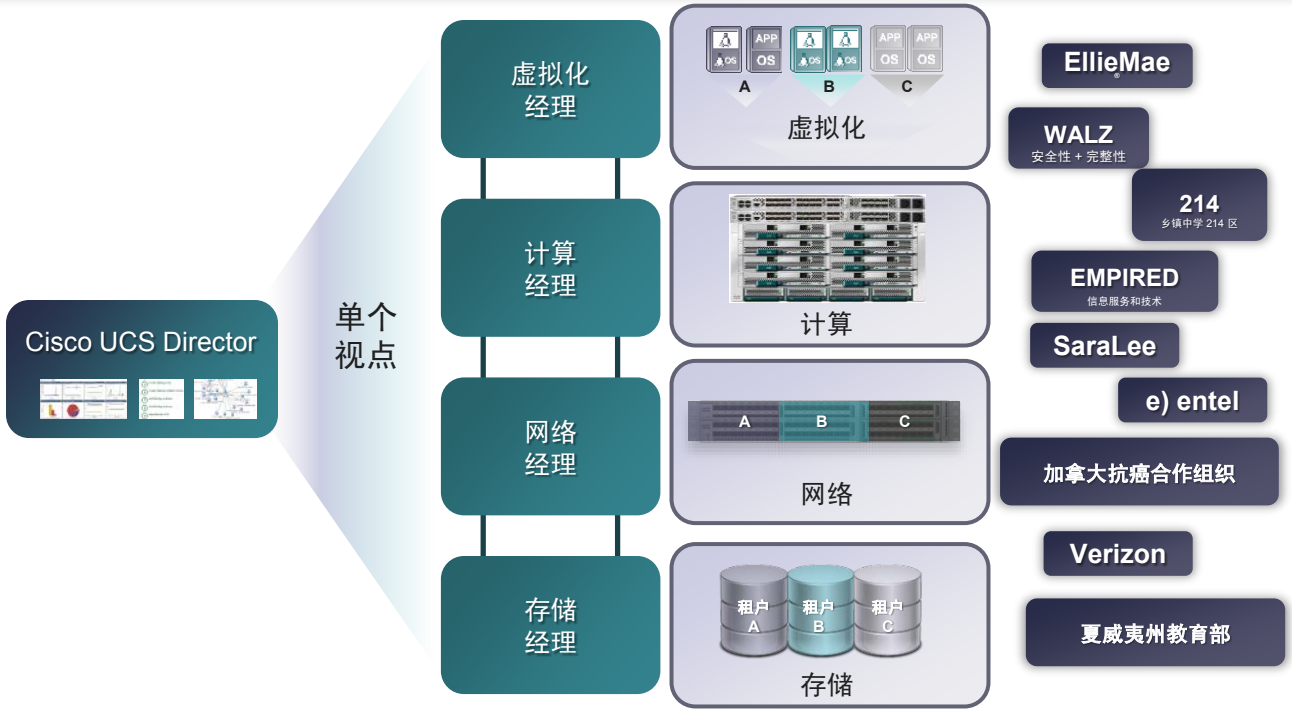
- 一种思科® 框架，适用于通过云进行高度安全、轻松的应用部署
- 将安全多租户 (SMT) 提升到新的水平
- 对于第 1 阶段：
  - 专注于通过自动化轻松进行部署
  - 超越 SMT 提高安全性
- 未来阶段：
  - 通过新的特性和功能不断改善框架
  - 通过异类云改善应用部署



Cisco UCS Director
自动化和基础设施管理

SVC awards 2013 FINALIST

- 随时可以运行的解决方案；可在数小时内使用
  - 单个集成的解决方案
  - 透明的虚拟和物理资源池
  - 与虚拟机监控程序无关
- 端到端自动化
  - 基于模型的自动化 – 不需要脚本
  - 策略驱动的一键调配
  - 持续的生命周期管理

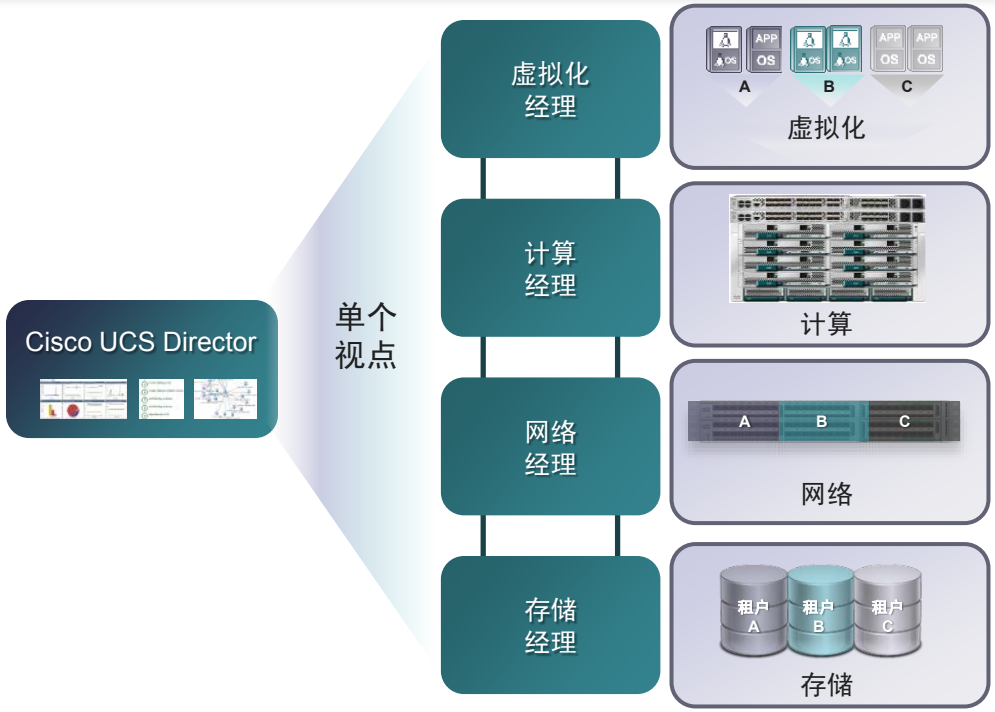


客户越来越多地购买作为单个融合系统提供的计算、网络、存储和虚拟化资源

Cisco UCS Director
自动化和基础设施管理

SVC awards 2013 FINALIST

- 随时可以运行的解决方案；可在数小时内使用
  - 单个集成的解决方案
  - 透明的虚拟和物理资源池
  - 与虚拟机监控程序无关
- 端到端自动化
  - 基于模型的自动化 – 不需要脚本
  - 策略驱动的一键调配
  - 持续的生命周期管理

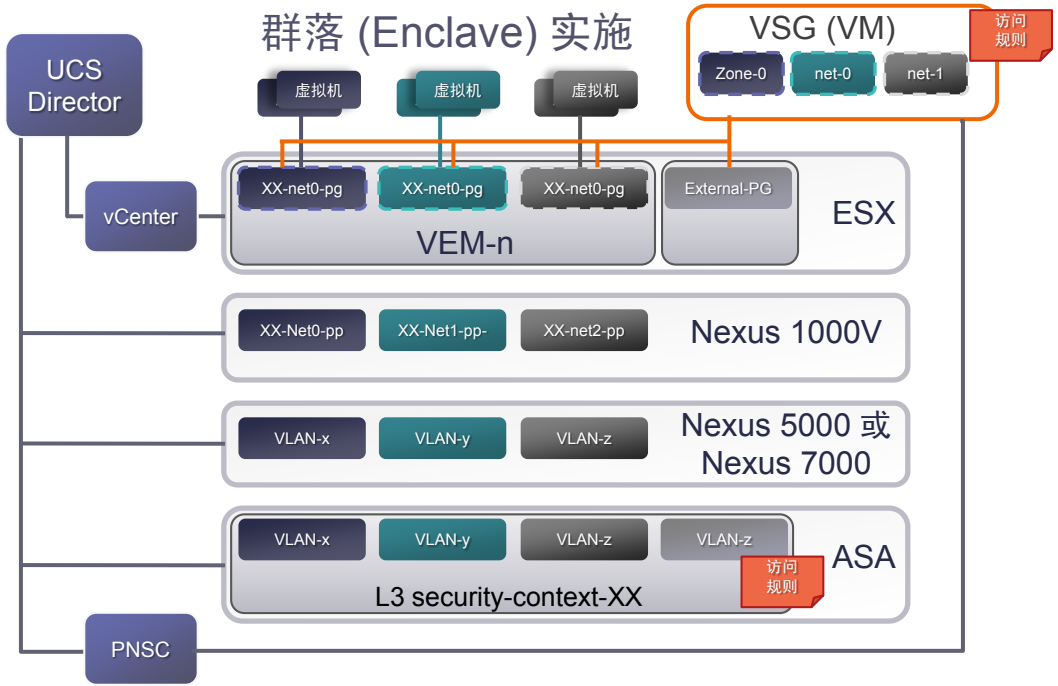


客户越来越多地购买作为单个融合系统提供的计算、网络、存储和虚拟化资源

安全群落 (Secure Enclave) 实施 - 拓扑示例

包含 Cisco Nexus® 5000、Cisco® Nexus 1000、思科虚拟安全网关 (VSG)
和思科自适应安全设备 (ASA) 的 vSphere

群落 (Enclave) 模型



思科认可设计流程

通过系统级设计和验证实现的创新和质量

重要的客户活动
请考虑端到端视图

领导理念
系统级创新

系统
开发基础

产品开发
跨平台协作

系统交付
经过测试和验证的设计

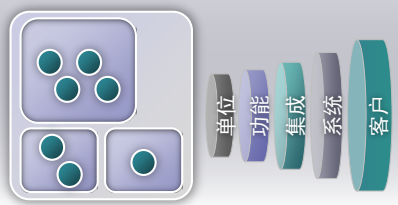
系统开发指南

Cisco Validated Design

规划

设计

端到端的验证

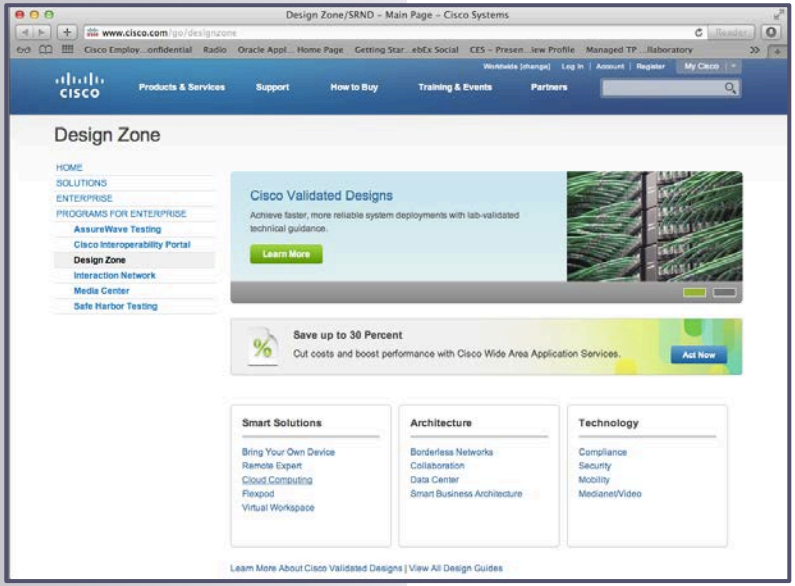


文档

设计区 – 思科认可设计门户

以下方面的设计和实施指南：

- 智能解决方案
- 架构
- 技术



http://www.cisco.com/go/designzone

小结

- 采用思科® 安全数据中心，为您的数据中心、分支机构和园区获得全面的端到端安全
- 更快、更轻松地部署安全策略
- 节省资金并提高运营效率
- 通过数据中心自动化更好地访问资源

谢谢各位。

集成解决方案
行业领导者的创新

垂直解决方案重点

医疗卫生 | 金融服务 | 制造 | 零售

应用

企业应用	数据库	业务分析/大数据	虚拟桌面
Oracle	Oracle	SAP	Citrix
Dedwards		Microsoft SQL Server 2008	Vmware
PeopleSoft	Microsoft SQL 服务器	Greenplum	Vmware View 5
SAP		HANA 和 BWA	Vmware ThinApp
Siebel E-Sales E-Marketing E-Service	My SQL	Hadoop	Citrix XenApp
Microsoft SharePoint		SAS	Citrix XenDesktop
Microsoft Exchange		Cloudera	Microsoft
		ParAccel	

管理

CISCO | BMC Software | Microsoft | Vmware | EMC² Where information lives | Solar Winds Unexpected Simplicity

CA | Cloupia | Symantec | IBM | HP | Zenoss | DynamicOps | Compuware The Technology Performance Company

操作系统和虚拟机监控程序

Windows Server 2008 Hyper-v | Redhat | Oracle Solaris | Enterprise Linux | Xenserver

Windows Server 2008 R2 | Open Suse | Vmware | Citrix | Oracle

智能解决方案

vBlock

FLEXPOD

VXI

RISC 迁移

集成解决方案
行业领导者的创新

垂直 解决方案重点	医疗卫生	金融服务	制造	零售
应用	企业应用：ORACLE、PeopleSoft、JD EDWARDS、SIEBEL、SAP、SharePoint 2010、Exchange	数据库：ORACLE、SQL Server 2008、MySQL	业务分析/大数据：SAP、SQL Server 2008、GREENPLUM、sas e-Intelligence、hadoop、cloudera、HANA & BWA、PARACCEL	虚拟桌面：CITRIX、vmware、vmware、ThinApp、CITRIX XenApp、CITRIX XenDesktop、Microsoft
管理	bmcsoftware、Microsoft、vmware、EMC²、solarwinds、DynamicOps、ca、cloupia、Symantec.、IBM、hp、Zenoss、Compuware			
操作系统和 虚拟机监控程序	Windows Server 2008、Windows Server 2008 Hyper-V、redhat、OPEN SUSE、ORACLE SOLARIS、Enterprise Linux、ORACLE、CITRIX、vmware、XenServer			

智能解决方案

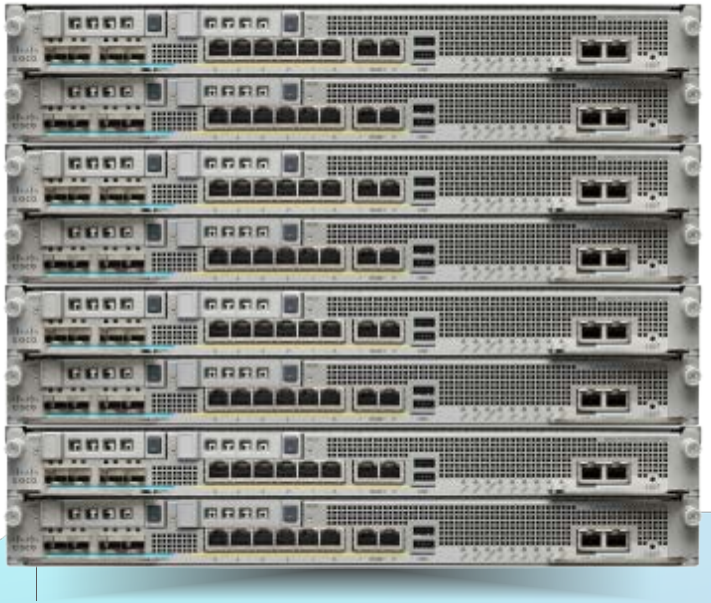
vBlock

FLEXPOD

VXI

RISC 迁移

网络性能得到提升



700% 更高的性能密度
- 每秒的新连接数可达 190 万个
- 每秒的最大连接数可达 8000 万个

84% 更低的能耗

87% 更小的机架空间

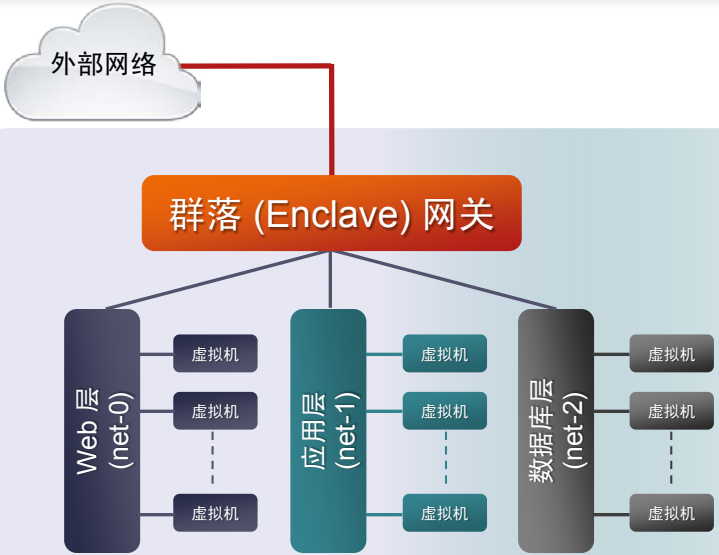
适用于高性能数据中心的下一代防火墙

SEA：
应用映射

允许 IN (HTTP/HTTPS)
全部拒绝

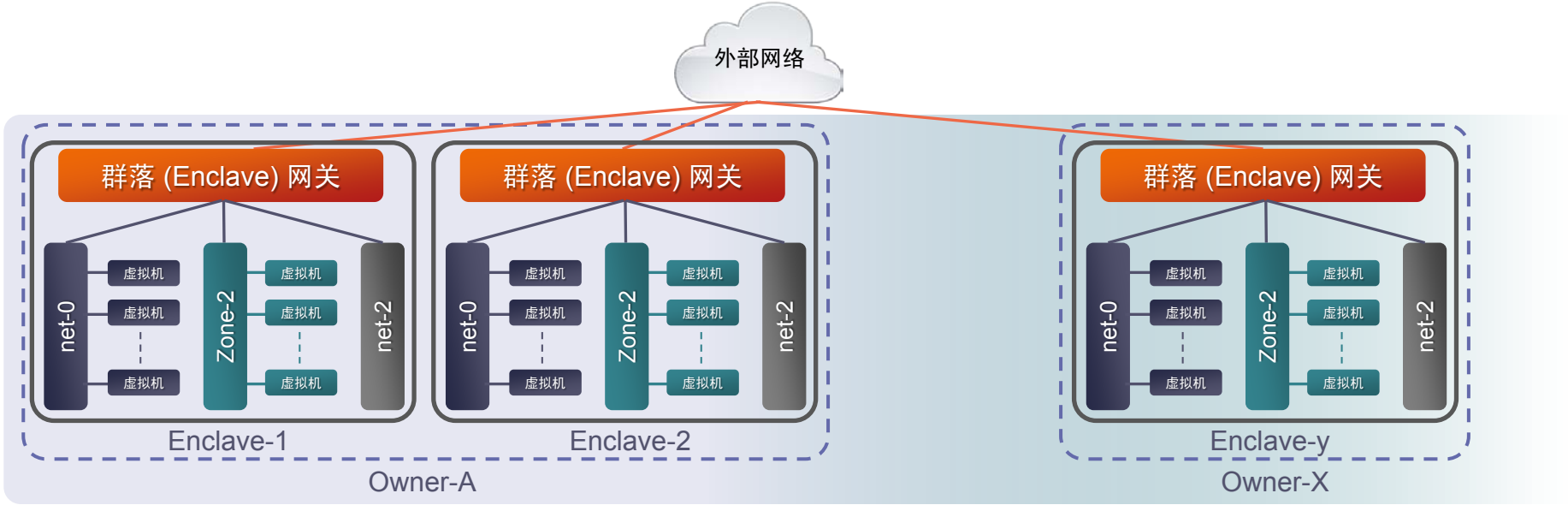
允许 IN（应用端口）
全部拒绝

允许 IN（数据库端口）
全部拒绝



- 将 HTTP/HTTPs 端口映射至 net-0 Web 负载均衡器 HTTP/HTTPs 端口
- 允许 net-0 -> net-1 应用端口
- 允许 net-1 -> net-2 数据库端口
- 拒绝所有 net-0、net-1、net-2

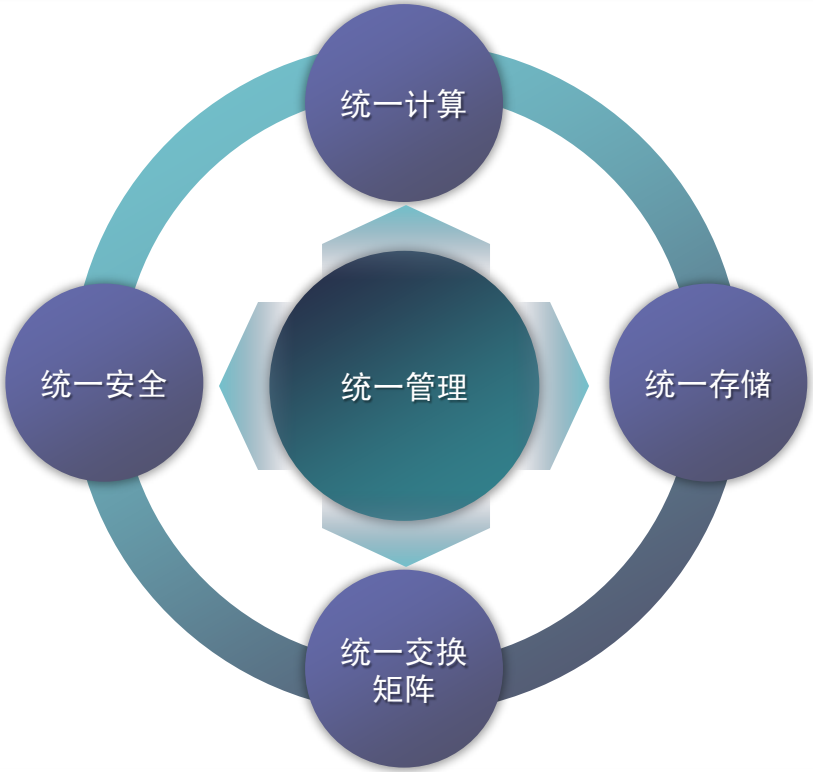
SEA：
扩展



- 可能托管成百上千个群落 (Enclave) 的共享基础设施
- 每个群落 (Enclave) 可以包含具有多层的一个或多个应用环境

- 每个群落 (Enclave) 扩展点取决于它使用的特定服务的可扩展性
- 利用 Cisco TrustSec® 技术优化群落 (Enclave) 之间的通信

Secure Enclaves Architecture
安全且自动化的应用云



- 将 HTTP/HTTPs 端口映射至 net-0 Web 负载均衡器 HTTP/HTTPs 端口
- 允许 net-0 -> net-1 应用端口
- 允许 net-1 -> net-2 数据库端口
- 拒绝所有 net-0、net-1、net-2