思科SAFE：下一代企业安全架构

为什么要使用经过验证的企业网络安全架构？

网络正在经历巨大的变革。诸如虚拟化、云计算和基于 Web 的访问等层出不穷的创新，正在为几乎每个组织的基础设施带来引人注目的变化。

从安全的角度来看，这些创新也伴随着很多新型的、复杂的安全威胁，它们会攻击网络和服务的可用性，滥用新应用和网络资源，以及盗窃数据和身份。传统的单点安全解决方案在很大程度上已经无法应付这些威胁。

企业需要经过实验检验的可靠指导，以便更好地保护这些新兴的关键业务服务，同时防范新兴的安全威胁。

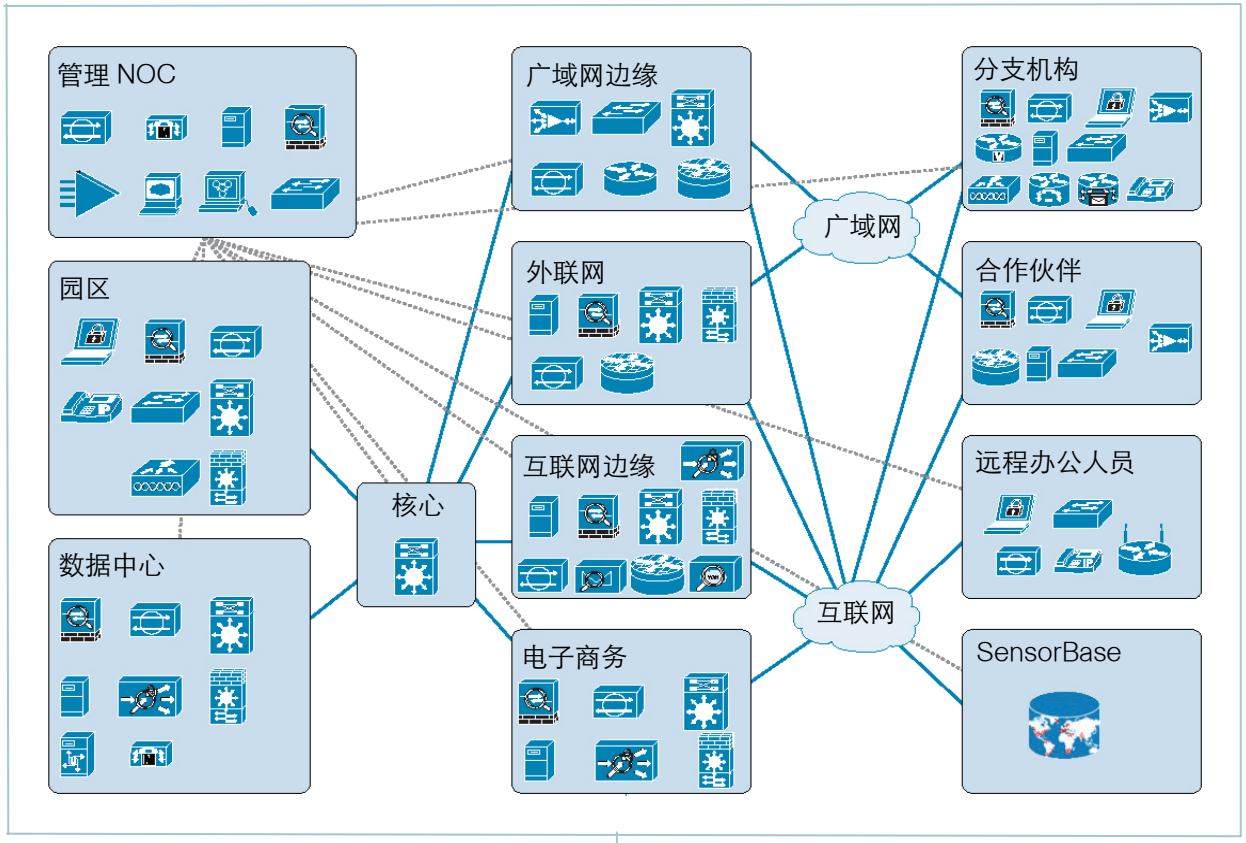
复杂的威胁和安全问题

当今各种复杂的新兴威胁日益将攻击目标锁定在特定网络，以及新技术和服务。这些威胁和问题包括：

- 越来越高明和有效的僵尸攻击
- 新兴的移动电话威胁
- 不断增多的恶意间谍软件
- 滥用 Web 应用
- 影响消费者设备的供应链攻击
- 日益严格的法律和法规要求

思科SAFE企业安全架构

作为一种企业安全架构，思科 SAFE 是思科验证设计计划的重要组成部分。SAFE 在最佳实践的基础上，提供了规范的设计指南，用以帮助用户规划、设计和部署安全解决方案。SAFE 的模块化设计可以满足网络中不同位置的特有要求，例如园区、互联网边缘、分支机构和数据中心等。



思科 SAFE 的深层防御架构蓝图提供了最佳实践来保护网络中的关键数据和事务处理。企业可以战略性地在整个网络中部署思科产品和功能，并充分利用安全和网络平台之间的协作优势。

思科 SAFE 设计着重于通过帮助企业开发和加强网络的可视性与控制能力，支持关键的业务和网络服务。

可视性

- 识别用户、服务、流量和端点，并进行分类
- 监控性能、行为、使用模式、事件和策略遵从性
- 收集、分析和关联整个系统中的事件

控制

- 增强端点、服务、服务器、应用和基础设施
- 在需要遏制威胁传播时，隔离用户、系统和服务
- 实施接入控制和安全策略，减轻安全事件的影响

思科SAFE：下一代企业安全架构

在此基础之上，思科 SAFE 为用户提供了一个经过验证的安全策略，能够确保不同网络位置之间和内部的交互与事务处理的安全，从而创造出一个高度安全的网络环境。

SAFE具有哪些优势？

思科 SAFE 架构可以就安全网络的所有方面提供指导，使企业能够根据可用的预算和重要需求，制定周密的安全部署策略。

- 循序渐进的网络安全设计和实施指南有助于缩短部署时间。
- 基于解决方案的方法重点关注风险管理，而不是产品放置。
- 分层安全设计有助于防止网络受到大规模或意外攻击的影响。
- 威胁可视性和协调一致的响应有助于降低风险和 IT 负担。
- 集成的安全和网络架构有助于确保关键业务服务的可用性。
- 模块化设计使企业能够根据优先顺序，逐步加强各领域的安全。
- 经过全面测试和验证的设计

除此以外，这些最佳实践和功能还可以帮助企业达到其合规要求。

思科安全生命周期服务

SAFE 服务基于生命周期方法提供，涵盖了整个生命周期流程：

战略和评估：思科提供了一组全面的评估服务，可帮助企业了解当前的安全状况和计划，以战略性地部署 SAFE 安全规则。

部署和移植：思科提供的部署服务可以帮助企业规划、设计和实施思科 SAFE 验证设计。

远程管理：思科远程管理服务提供的工程师和工具能够前瞻性地监控 SAFE 安全基础设施，24x7 全天候提供事件、故障、变动、配置和报告服务。

安全情报：思科安全情报运营服务可以提供预警情报、分析和经过实验检验的威胁规避技术，以帮助安全专家应对层出不穷的威胁。

安全优化：思科安全优化服务是一种集成的服务方案，旨在通过每季度一次的站点考察和持续的分析调试，评估、建设和优化企业的安全基础设施。

了解更多信息

如需了解更多关于思科 SAFE 的信息，请联系您当地的客户经理或安全产品销售专家，或者请访问：http://www.cisco.com/go/safe。您还可以访问 www.cisco.com/go/cvd，免费下载 SAFE 设计和实施指南。

如需了解关于思科安全产品和服务的详细信息，请访问：http://www.cisco.com/go/security。如需了解关于思科安全服务的详细信息，请访问：http://www.cisco.com/go/services/security。

C45-526808-00 03/09