思科安全分区服务

通过高度安全的区战略降低风险

用户、应用和系统之间的网络和交互异常复杂。这使安全团队更难保护数据和系统的机密性、完整性和可用性。传统的安全方法无法满足这种全新技术领域的需求和规模要求。此外，它们也无法提供有效控制和监控所需的一致性、可扩展性和相应的详细信息。

思科® 安全分区服务提供战略性的基础设施分区方法。它使像你们一样的组织在今天超连接的复杂环境下，可以降低风险、简化审核配置文件、保护数据和应用，并且能实现更高级的防御，以满足董事会级的要求。

优势

- 制定与业务目标匹配的高度安全的分区战略
- 降低组织的数据和资产的风险。
- 在多个安全领域运用有效的安全和策略控制。
- 保护数据和知识产权，防止受到内部和外部网络攻击

案例研究

美国公共部门

挑战

- 客户在缺乏网络分段的扁平网络上操作，这给他们的环境带来了安全风险

解决方案

- 思科使用基于软件的解决方案来集成物理安全和信息安全。
- 通过将城市的 3 个不同区域指定为高、中和低风险区来创建多个分区

成果

- 改进的合规性和一致的详细工作流程提高了策略、标准和程序的可用性
- 改进了网络安全威胁、风险和漏洞的可视性

全新的分区方法

这是一种新的分区方法，更全面地考虑业务和应用影响，以及特定的垂直设计模式。我们的方法围绕客户的具体情况，超出网络范畴，并且包含可重用的设计模式。

思科安全顾问与您配合，可以识别定义环境内安全区的关键参数。必要时，他们会考虑和采纳各种基础设施分区设计模式，包括具有以下特点的设计模式：

- 垂直行业的共同点
- 基于业务部门或行业进行划分
- 适用于保护地理边界
- 以拓扑为中心（例如，远程站点与数据中心）
- 基于上述方法的混合方法

经验丰富的专业人员

作为战略技术顾问，思科安全咨询服务团队帮助业内领先的组织识别信息安全方面的战略机会。我们帮助您保护网络性能、创造竞争优势，并且获取长期可持续的业务价值。有优质资源组合做后盾 - 大量研究和威胁情报、成熟的方法，以及安全、云、移动、协作和数据中心运营方面的多学科专家 - 我们的客户能够更好地管理风险和合规性、开发强大的安全评估、控制成本，并实现战略 IT 和业务目标。

后续行动

思科安全分区服务是思科安全咨询服务产品组合的一部分。我们的安全顾问能够帮助您的组织制定强大的安全、合规和威胁管理策略。要了解有关安全分区服务如何惠及贵企业的更多信息，请联系您的当地客户代表或授权思科经销商。如需详细了解思科如何帮助您的组织防御当今不断变化的威胁，请访问 cisco.com/go/services/security。