Cisco Defense Orchestrator

轻松实现高效的安全管理

在当今复杂的扩展架构中，管理网络安全是一项艰巨的任务。面对狡黠的攻击者，您需要处处实施安全控制，全面覆盖您的数据中心、私有云、公共云、远程站点和移动员工。

通常，这意味着要使用多个控制台和多种策略结构，来监控各种传统设备和下一代设备。在这样的环境中，更新、升级和部署过程既单调又耗时。不仅如此，效率低下的工具和流程还有可能引入漏洞并增加入侵风险。

这种复杂的策略管理方式可能会影响组织效率和安全防护效果。

Cisco® Defense Orchestrator 是基于云的应用，可对思科安全产品实现一致的策略管理。它能够以简驭繁，让您轻松抵御最新的网络威胁，节省您的宝贵时间。

益处

- 降低复杂性：简化安全策略和设备管理
- 节省时间：提高重复性安全任务的执行效率
- 增强安全性：实现更出色、更一致的安全性

主要功能

扩展和集中 – 只需编写一个策略，即可在整个网络中将该策略的实施一致地扩展到成千上万个安全控制点。通过单个集中式控制台比较、过滤、编辑和新建策略。

分析问题 – 分析整个网络中的现有安全策略和对象，发现错误和不一致。轻松更正问题，从而增强安全态势，优化设备性能。

提升部署速度 – 创建标准策略模板，为您的思科环境提供一致、有效的保护，从而更快地安装和配置新设备。新部署的设备会自动继承更新后的策略。

轻松升级 – 快速更新安全补丁并获取新功能。只需点击几下即可完成防火墙软件映像升级。可实时执行任务或预约执行时间。

更加智能的配置管理 – 每项更改都记录在更改日志中并可查看。可随时回退到最近的已知正确配置。

© 2019 思科和/或其附属机构。版权所有。

案例研究：Cisco Defense Orchestrator 将升级时间从一整天缩短到半小时

某组织需要更新网络中的 40 个思科自适应安全设备 (ASA) 防火墙的固件。网络运营经理告诉我们，她通常要抽出一整天、有时甚至更长的时间来规划、部署和监控项目。借助 Cisco Defense Orchestrator，她在 30 分钟内完成了升级，节省的 7 小时 30 分钟可投入到优先项目中。

支持的平台

Cisco Defense Orchestrator 构建在一个开放式平台上，该平台支持以下产品的安全策略管理和配置：

- Cisco ASA 5500-X
- 思科自适应安全虚拟设备 (ASAv)
- Cisco Firepower® 下一代防火墙 (NGFW)
- Cisco Firepower Threat Defense (FTD)
- Cisco Meraki MX

简化、统一和协调

长期以来，跨众多思科安全设备管理安全策略是一项巨大挑战，而 Cisco Defense Orchestrator 解决了这个问题。得益于以下特点，它能减轻您的工作负担：

简单。Cisco Defense Orchestrator 能够简化安全策略管理和设备管理。它基于云，可以随时设置并开始运行，为您和您的企业立即带来价值。

高效。用于重复性安全管理任务的时间减少多达 90%。

有效。Cisco Defense Orchestrator 可确保变更已被执行且策略保持一致。虽然它无法杜绝人为错误，但可以帮助纠正错误。

Cisco Defense Orchestrator 能够无缝地统一策略并协调变更。它提高了一致性，降低了复杂性，由此增强安全性。

“Cisco Defense Orchestrator 的云功能非常容易使用。我们在安全策略管理任务上花费的时间至少节省了 75%。”

– Robin

某企业电信服务提供商的安全官

© 2019 思科和/或其附属机构。版权所有。

后续行动

目前，北美和欧洲有数百家客户已开始使用 Cisco Defense Orchestrator。详细了解它如何帮助您简化安全策略管理、提高团队效率并增强安全性。

立即访问 cisco.com/go/cdo 或发送邮件至 cdosales@cisco.com。

© 2019 思科和/或其附属机构。版权所有。Cisco 和 Cisco 徽标是思科和/或其附属公司在美国和其他国家/地区的商标或注册商标。要查看思科商标列表，请访问以下网址：https://www.cisco.com/go/trademarks。文中提及的第三方商标为其相应所有者的财产。“合作伙伴”一词的使用并不意味着思科和任何其他公司之间存在合作伙伴关系。
(1110R) C45-736943-03 05/19