

企业内网络细分

简化零信任细分而不中断业务

数字化转型效率、创新和生产力的承诺带来了扁平的互连网络，这些网络容易受到威胁横向移动的影响，而且对于越来越多的连接物联网企业 (EoT) 及扩展企业，也无法确保其安全。当 IT 团队探索细分方案以实施零信任控制并提高安全性时，对于复杂的部署和昂贵的业务中断的担忧挫败了组织的信心，阻碍了进展。挑战包括：

- 缺乏推进细分项目的信心
- 数字化转型带来的威胁和暴露风险
- 多供应商运营的复杂性和多域环境中细分政策的不一致性
- 缺少技能、资源和工具，无法在扩展企业有效地设计、建立和部署网络细分

为何选择Fore Scout: 同类最佳解决方案，实现非破坏性零信任细分

如果这些挑战听起来很耳熟，那么现在就是评估Fore Scout解决方案的绝佳时机，该解决方案简化了零信任细分，优化了您的互连EoT在扩展环境中的风险管理。Fore Scout平台加速了动态的、情境驱动的网络细分，而不会为企业提高复杂性、增加成本或造成负面影响。

“IoT和支持网络的设备技术为网络和企业带来了潜在的危害……安全团队必须持续对网络上的每个设备进行隔离、确保安全和控制。”¹

FORRESTER RESEARCH
2020年6月

我们将通过以下方式帮您满足需求：

- **加速扩展企业中的零信任细分**
- 在任何设备、任何地点**立即实时了解网络细分状态**
- 通过IT、IoT和IoMT (医疗物联网) 系统之间的动态细分，**减少受攻击面，保持合规**，可以轻松满足不同的垂直环境需求
- 使用更少的工具、更少的仪表板和更多的可操作警报来**简化威胁分析**
- **通过有效管理网络安全检测和响应，降低合规风险和成本**，需要的技术资源也较少
- **优化跨团队的工作流程**，利用整个企业现有的投资和一致的细分策略

Forescout认识到，网络细分没有一个放之四海而皆准的解决方案。所有的细分工具都有特定的优势、用例和网络上的最佳部署区域。Forescout平台 (包括Forescout eyeSegment) 将这些不同的技术连接起来，加速整个扩展企业动态网络细分的设计、规划和部署，实施有效的零信任策略，降低监管风险并限制受攻击面。

扩展您的安全和IT投资价值

- 启用非破坏性的动态细分
- 加速网络零信任细分项目，满怀信心
- 减少业务中断的风险
- 降低运营成本
- 迅速适应合规和监管要求
- 利用现有的基础架构投资

消除零信任分段的复杂性

如下图所示，企业内的细分需要一个情境驱动的多层架构，以应对当今设备类型广泛的多样性，无论它们从哪里连接到网络。Forescout提供平台、工具和专业技术帮助您有效规划和实施这一解决方案。



解决方案组件

Forescout平台帮助组织设计其企业内的网络细分、战略并加快部署。以下是该平台的主要产品：

Forescout eyeSight：每个IP地址的丰富情境

eyeSight产品为整个连接网络（从园区到数据中心再到云端）提供了无与伦比的洞察和情境——将您的连接清单转化为设备、应用程序、用户和服务的逻辑分类法。使用此分类法将所有连接的设备归入一个逻辑业务层次结构，用于网络细分。访问 <http://www.forescout.com/platform/eyeSight> 了解更多详情。

Forescout eyeSegment：简化任何设备、任何地点的零信任细分 Forescout eyeSegment可加速整个扩展企业的动态零信任细分的设计、规划和部署。eyeSegment使企业能够为EoT安全接受零信任原则。eyeSegment能够快速加速整个扩展企业的细分项目，减少受攻击面，限制爆炸半径，并缓解监管和业务风险。访问<http://www.forescout.com/platform/eyeSegment> 了解更多详情。

eyeControl/eyeExtend：在网络管区和多供应商环境安排一致的控制

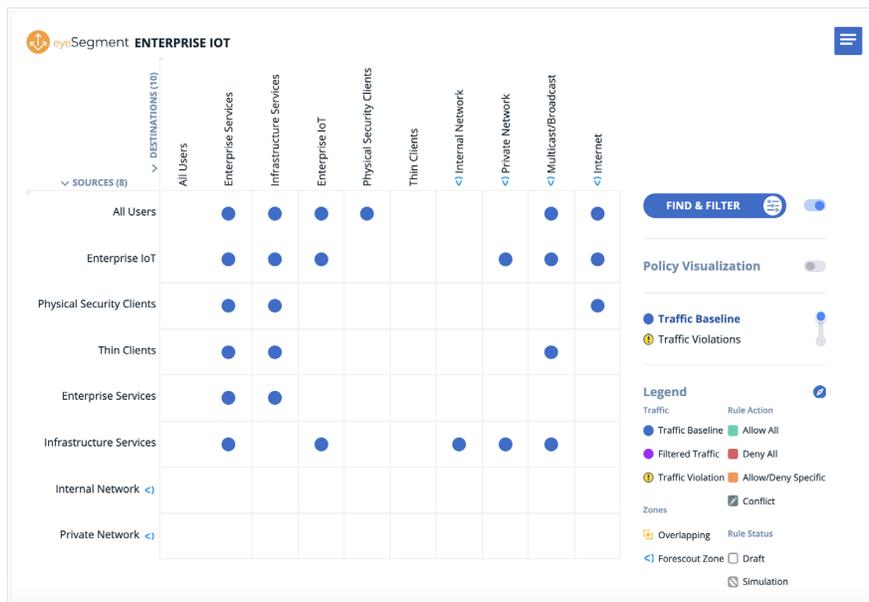
Forescout平台通过利用Forescout

eyeControl和eyeExtend产品，让您能够动态协调细分策略，并在异构执行技术之间实现自动化控制。

- eyeControl使情境感知的细分策略和控制能够一致地执行到现有的基础技术中——消除了对代理的需求。若要了解更多请访问 www.forescout.com/platform/eyecontrol
- eyeExtend产品通过与领先的下一代防火墙（NGFW）供应商进行开箱即用的集成来协调控制。访问 www.forescout.com/platform/eyeextend 了解更多关于Forescout NGFW集成的信息

可视化流量以了解策略设计

Forescout细分解决方案让您专注于对您而言很重要的事情，这样您就可以分析和调查环境中的特定流量模式，如上图所示。您可以立即了解通信流的当前状态，并创建所需的零信任细分策略。这个可见性优先的方法让您轻松地建立微细分区域，在确保业务连续性的同时保护您的业务。



用例

Forescout网络细分解决方案解决了不同垂直行业的广泛用例，如医疗、OT (运营技术)、金融服务、政府、零售等。在每个案例中，Forescout平台的灵活性都有助于降低业务中断的风险，并最大限度地减少与零信任实施和细分项目相关的运营成本。若要了解更多用例，请访问企业内网络细分用例概述。

总结

由于跨域技术的复杂性，目前细分项目都是孤立管理的。额外的因素，如零信任安全、数字化转型和监管合规性，需要一个更全面和系统的方法。Forescout解决方案解决了组织在扩展企业中跨域、多用例的细分挑战。通过立即实时了解您的“当前状态”细分、情境感知策略、业务结构组和主动策略模拟，Forescout平台可实现跨越不同执行技术的零信任细分控制，并验证预期结果。最终结果是快速加速零信任细分项目，包括更精细的控制和降低整个组织的风险。

¹用零信任减轻勒索软件的影响，弗雷斯特研究公司，2020年6月8日

网络细分研讨会

您是否在将您Forescout部署扩展到高级细分控制场景？

现在Forescout的顾问提供了一个网络细分研讨会，确保您的网络细分策略和实施与您的业务战略一致。[了解更多。](#)

不要视而不见。
要保护。

马上联系我们，主动保护您的物
联企业。

forescout.com/solutions/network-segmentation

china@forescout.com

zh.forescout.com

 **FORESCOUT**
Active Defense for the Enterprise of Things™

Forescout Technologies, Inc.
190 W Tasman Dr.
美国加利福尼亚州圣何塞，95134

电子邮件 china@forescout.com
电话 (国际) +1-408-213-3191
支持+1-708-237-6591

[访问Forescout.com](https://www.forescout.com) 了解更多

© 2020 Forescout Technologies, Inc. 保留所有权利。Forescout Technologies, Inc. 是一家特拉华州公司。访问 www.forescout.com/company/legal/intellectual-property-patents-trademarks，查看我们的商标和专利列表。其他品牌、产品和服务的名称可能是其各自所有者的商标或服务标志。
版本 08_20