# Forescout eyeExtend Connect

## 轻松与Forescout平台集成，获取上下文设备见解并加快企业范围的威胁响应

为了增加安全和IT技术投资带来的价值，Forescout的客户一直在利用包含九种常用安全技术产品的现成集成。这些集成通过安全工作流的编制极大地提高了效率。除了这些预建产品之外，Forescout目前还为需要将更多现有技术与Forescout平台集成的客户提供了一种更加快捷轻松的方法。

eyeExtend Connect是Forescout的新产品，可以使我们的客户和伙伴社区快速地构建、使用和共享连接起Forescout平台与其他技术的eyeExtend应用。这允许社区利用Forescout的深度设备上下文来释放现有安全产品的价值，在不同的解决方案中自动执行安全工作流和强制执行策略，并加快系统范围的响应速度以降低风险。

## 解决方案

Forescout eyeExtend Connect简化了应用创建过程，易于使用和部署。您可以通过Forescout eyeExtend应用轻松地将Forescout平台与您的IT和安全技术集成，并编制各种网络安全技术的安全工作流。

凭借eyeExtend Connect，您目前的安全技术可以利用Forescout eyeSight的深度设备上下文数据，包括设备属性、安全状态、设备与公司策略的合规性、网络位置、用户上下文等。此类设备数据可以由其他IT或安全产品自动提取，也可以由设备自行推送至Forescout平台。eyeExtend Connect还可以让您自动执行系统范围内基于策略的操作来减少威胁、事件和合规性差距，从而有助于加快威胁响应速度。

eyeExtend Connect提供以下工具，以实现工作流编排和

设备上下文共享。

eyeExtend connect

### 挑战

- Forescout或技术伙伴提供的预建集成产品与使用其他内部安全技术的工作流编制相互排斥
- 自定义构建集成的开发周期较长，增加了实现当前安全投资价值的时间

  安全工具在不共享设备和用户上下文的情况下独立工作，
- 在响应安全事件时需要大量手动工作，从而导致网络风险增加和生产力下降

### 优势

- 与所有类型的第三方工具集成，最大限度地提高当前技术投资的回报
- 通过eyeExtend应用轻松快速地与Forescout平台集成，更快地实现价值
- 使您的IT和安全工具更好地协同工作，更快地获取可行性设备见解并自动解决风险和威胁，从而提升安全状态

## 亮点

- 轻松构建和部署eyeExtend应用，与开放的Forescout平台集成
- 与社区共享您的应用，提供信息并寻求反馈
- 使用Python脚本和JSON配置构建便携式应用
- 与广泛的第三方Web服务集成
- 使用第三方设备上下文和控制扩展Forescout可见性和控制性
- 使用基于开放标准的REST API实现双向集成
- 将信息推送至和拉取出标准结构化查询语言（SQL）
- 生成自定义查询，将信息推送至和拉取出标准轻型目录访问协议（LDAP）服务器
- 通过syslog向指定服务器发送和接收信息

## eyeExtend应用

构建应用，利用Forescout平台的关键功能来学习和共享端点上下文、采取网络控制操作并强制执行系统范围的策略。eyeExtend Connect提供了易于使用的JSON模式，可供定义参数、标签和用户控制的配置，让您的eyeExtend应用实现便捷迁移

（从测试迁移至生产、从区域A迁移至区域B、从IT环境迁移至OT环境等）。此外，第三方API交互是使用常用的Python脚本定义的，这些脚本可以扩展可构建的集成类型，提供极大的灵活性。重要的用例和强制执行（例如威胁缓解、事件响应和合规性管理）可以通过应用中内置的策略模板实现自动化。

eyeExtend应用的主要功能：

- 即插即用
- 发现新的设备和属性
- 外部第三方控制操作
- 自定义策略模板
- 可编脚本的API交互
- 可自定义的第三方图标

**WebAPI和数据交换（DEX）**

Forescout平台提供了一组RESTful API，使外部应用可以检索Forescout设备属性和策略信息。DEX（数据交换）插件支持Forescout平台和第三方RESTful API之间的双向通信，以共享实时设备上下文。

**结构化查询语言（SQL）**

DEX插件能够将信息推送至和拉取出标准SQL数据库。此类集成允许自主开发的应用与

能够通过外部或内部数据库连接的第三方产品共享信息。您可以在外部数据库中查询信息，并创建主机属性来存储Forescout平台检索的数据。这些主机

属性可在Forescout策略中使用，并可在网络操作系统（NAC）和清单视图中查看。您还可以根据Forescout平台收集的信息来更新外部数据库，这些信息通常供第三方产品使用。

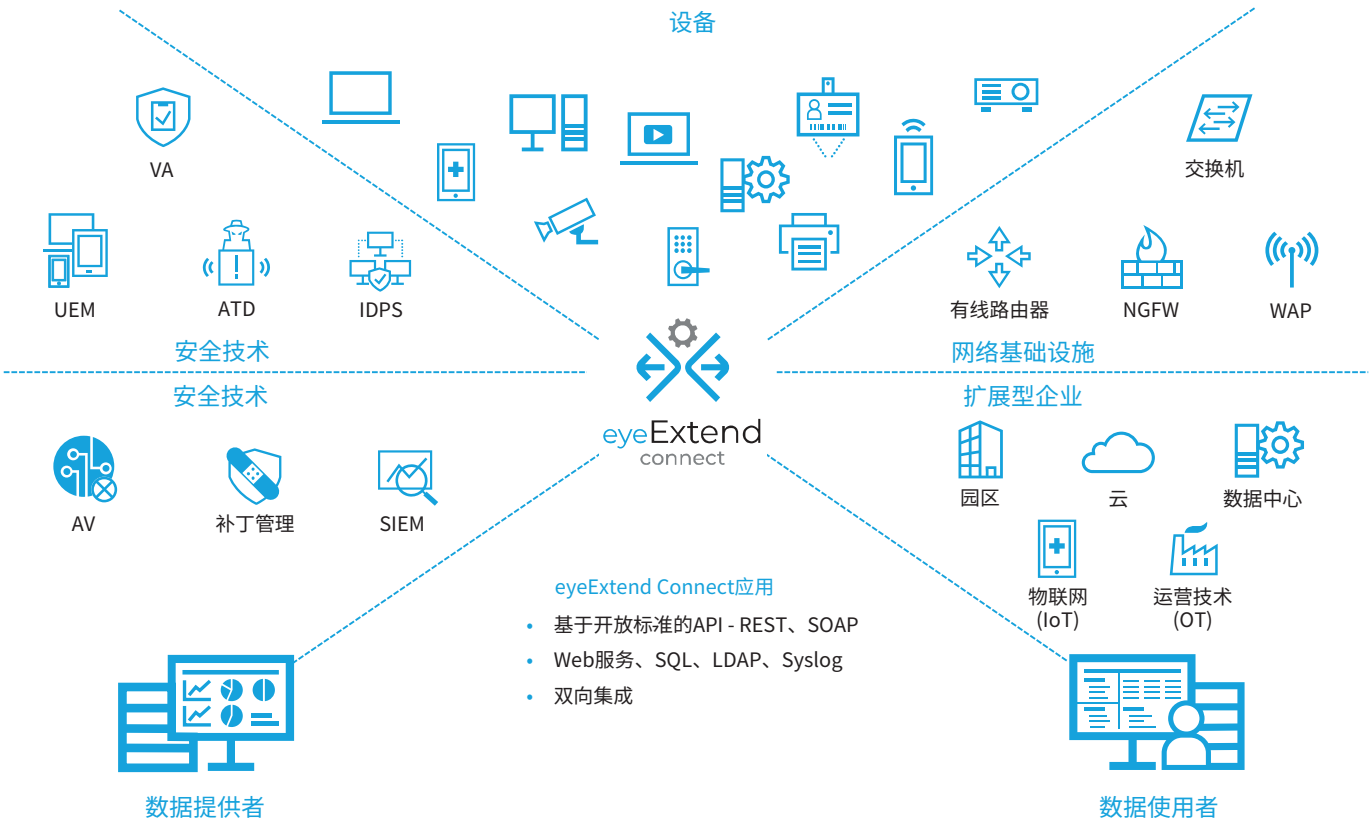
**轻型目录访问协议（LDAP）**

通过DEX插件生成自定义查询，将信息推送至和拉取出标准LDAP服务器。例如，您可以在LDAP服务器上查询信息，并创建Forescout主机属性来存储已检索的数据。这些主机属性可在Forescout平台策略中使用，并可在NAC和清单视图中查看。

### Syslog

DEX插件可以配置为通过syslog向指定服务器发送和接收信息。此类接口可用于与聚合日志并支持日志分析的产品（例如安全信息和事件管理（SIEM）产品）进行多种集成，或与其他以此方式发送和接收警报的解决方案集成。可自定义消息格式。

图表1：跨不同设备、环境和安全技术编制工作流




VA：漏洞评估，ATD：高级威胁防护，IDPS：网络入侵防护，UEM：统一端点管理，
AV：防病毒，SIEM：安全信息和事件管理，WAP：无线接入点，NGFW：下一代防火墙

## 一般用例

Forescout提供了25种现成的解决方案来解决特定用例，同时eyeExtend应用可用于解决客户的自定义用例。以下是几个示例：

**立即发现、分类和评估连接网络的每台设备**

Forescout eyeExtend Connect由Forescout eyeSight提供支持，允许集成的IT或安全产品提供上下文，从而更好地识别整个企业中的设备，包括园区、数据中心、OT和云环境。例如，

Ubiquiti版的eyeExtend应用帮助客户提高其Wi-Fi连接设备的可见性，并利用客户发现的设备属性在Forescout平台中更好地做出策略决策。Ubiquiti版eyeExtend应用现在可以将Ubiquiti Wi-Fi连接的设备信息提供给另一个IT服务管理（ITSM）或资产管理产品，以完善客户的CMDB。另一个重要的应用是Google云端平台版的eyeExtend应用，它通过与Google云端平台集成并拉取Google云端平台的清单上下文，帮助客户实时可见其不断发展的云计算实例。

**提升对连接VPN的设备访问网络的可见性和控制**

eyeExtend Connect可以发现通过VPN连接到公司网络的所有设备。安全操作员可以利用与Forescout平台的集成，确定通过VPN连接的资产是否属于公司资产，并控制从未授权位置连接的设备的访问。

**编制安全或IT策略违反信息工作流**

使用不同的协作和消息平台发送违反策略的实时警报。您可以设置策略，允许在做出自动执行网络控制操作的策略决策时，通过电子邮件、消息或协作平台从Forescout平台获取设备事件数据。例如，Slack版的eyeExtend应用与协作平台集成，可将违反策略的实时警报发送至IT或安全团队使用的Slack渠道。

**自动执行移动设备注册，提升安全管理并强制持续合规性**

eyeExtend Connect与UEM系统编制设备信息共享和控制操作，为您网络上的设备提供统一安全策略管理，适用于任何设备类型（电脑、Mac、Linux®、平板电脑、智能手机）、连接（有线、无线、VPN），或设备所有权（公司或个人）。这种全面的设备管理可实现设备注册的自动化、通过策略驱动的操作强制设备合规性、自定义网络访问控制的应用，以及加快响应操作和补救措施。例如，客户现在可以借助Google移动管理版的eyeExtend应用，查看Chromebook的设备上下文。这些数据有助于完善公司自带设备（BYOD）的安全和访问策略。

**实现IT和安全产品生态系统内的操作和工作流自动化，可以改善整个企业内的运营并增强安全性**

eyeExtend Connect可以发送或接收用于指示Forescout平台或其他集成产品采取特定操作的操作触发器。此类触发器是基于策略驱动的自动化，无需人工操作员做出基于playbook的决策。这意味着在整个企业内响应时间更快、网络更加安全。

**利用深度上下文设备数据进行关联分析以加快事件响应速度 |**

eyeExtend Connect使Forescout平台能够将深度设备数据输入SIEM系统以进行关联分析。这种分析提供了整个企业攻击面的完整情况，有助于缩短见解时间和促进调查。Forescout平台还可以通过自动执行基于策略的操作来简化安全操作，根据SIEM实时反馈的事件严重性来限制设备对网络的访问。

总体而言，eyeExtend Connect将安全工具从孤岛中移出并将其接入高度智能的Forescout平台，
显著提升威胁缓解和策略合规性的自动化，从而帮助您快速实现更高的安全投资回报。

注意：eyeExtend Connect的某些功能以前是OIM产品的一部分。所有以前的OIM功能现在都是eyeExtend Connect的一部分。

FORESCOUT

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

免费电话（美国）：1-866-377-8771
电话（国际号码）：+1-408-213-3191
支持电话：+1-708-237-6591

访问 www.Forescout.com，了解更多信息