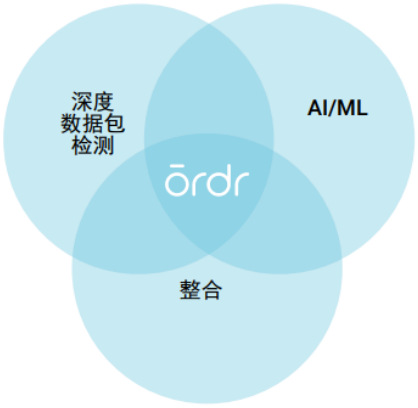
规模化提供资产可见性

使用深度包检测，人工智能和机器学习来提高设备识别的准确性

准确、持续的资产连接可视化是网络净化的基础。 如果可以根据设备的制造商、位置、操作系统、序列号和应用程序/端口使用情况对它们进行了正确分类，则可以实时了解到连接到您的网络的设备，并且确保对设备或环境的无感知，这个至关重要。 这需要显示资产唯一标识和属性的技术支持。

Ordr利用深层数据包检测（DPI）技术，该技术不仅分析数据包头，还分析其通信流的应用层，检索关键标识符以将其基于业务或操作功能分类并分组。

传统的网络访问控制（NAC）供应商试图在没有DPI的情况下实现类似的功能，并且客户会立即注意到完全利用DPI的技术与主要依赖非DPI遥测数据的技术之间的明显差异。



DPI和非**DPI**之间的根本区别是能够查看关键设备标识符，例如：

- 产品型号名称（非型号类型）
- 序列号
- 操作系统和软件版本
- 医疗器械形态类型
- 检查细节
- 设备利用率统计
- 数字证书
- 用户登录/注销模式
- 准确跟踪管理协议，例如SNMP、RDP、FTP、SSH等

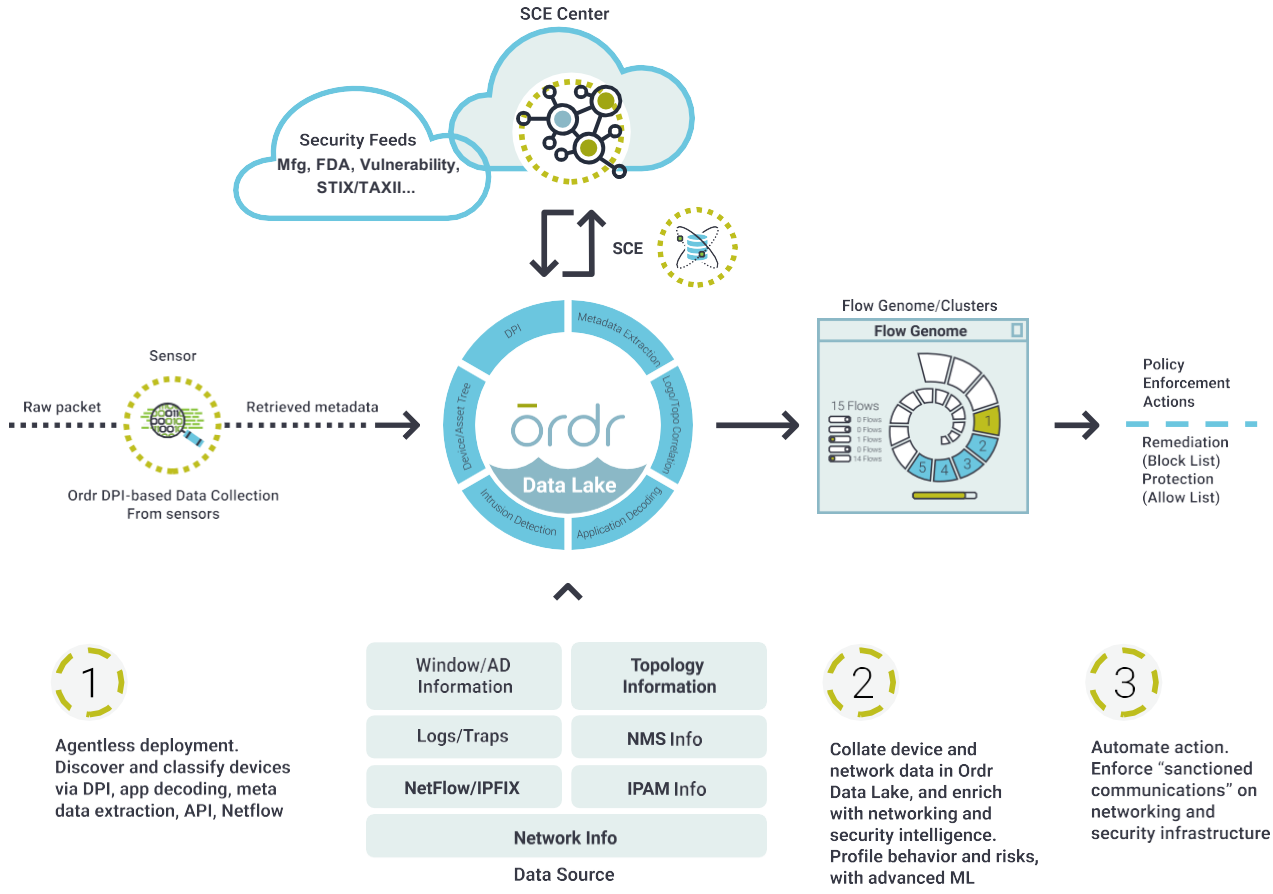
非DPI技术将不会揭示在应用程序层有效负载中更深处存在的此类数据。 如果分类过程中缺少此类标识符，将很难评估网络安全风险，因为您无法自信地判断您的设备是否具有与操作系统/补丁程序级别相关的特定漏洞，或者制造商披露的内容。 将公开的常见漏洞和披露（CVE）和通用漏洞评分系统（CVSS）信息与网络中设备的OS级别相匹配将是一项挑战。

Ordr系统控制引擎（SCE）平台及其高速无源数据包扫描技术还利用来自多个知名提供商的威胁源提供入侵检测系统（IDS）功能。Ordr的IDS功能监视器可监视活动威胁，并结合已知的漏洞检测功能，Ordr的DPI功能使我们的平台在业内无与伦比。

数字化转型带来了由连接的设备生成的大量数据，并且随着这种巨大的增长，许多组织都遇到了缺乏真正的网络可视化的情况。 IT部门过去常常负责所有托管资产，但是如今，组织有多个团队负责设备，这留下了巨大的空白和不可避免的非托管设备。 仅DPI不足以完成Ordr分类引擎， DPI分解设备流量并收集关键数据。 Ordr SCE平台使用其学习算法对具有相似特征的设备进行分组。 此类学习算法使Ordr平台可以了解关联一个设备与另一个在不同位置的设备，并创建紧密匹配。

人工智能（AI）和机器学习（ML）是Ordr平台中的另一关键技术，无论部署类型，内部部署还是在云中，都可大规模支持数十万个IT，OT和IoT设备。

通过自动训练分类模型来最大化DPI输出



在典型的工作流程中，来自设备的流量会发送到Ordr传感器，在那里大量流量会被解析并移交给Ordr DPI引擎。 每件数据都按属性分类（每个设备300～400个属性），并推送到Ordr Data Lake进行AI / ML处理。 在AI / ML流程内部，数据经历了诸如特征修剪、聚类和分类之类的阶段。 Ordr客户将其视为一个巨大的优势 - 整个过程的自动化可以提取大量连接到网络的不同设备类型，并提供最佳数据的工作流支持。 这正是单独DPI技术无法扩展的原因，也是Ordr成为DPI和AI / ML技术的领导者的主要原因。

该平台会持续训练其模型，以识别设备之间的相似性。 没有AI / ML技术，就不会全局化地学习设备。 它了解OS类型、版本、固件版本、型号名称、通信模式、流量目地、应用程序类型等方面的相似性。

通过集成丰富其他数据

我们已经看到很多情况下DPI由于各种原因而看不到或看不到足够的数据。 它可能基于网络的构造方式，也可能是设备本身未发送足够的数据。 摄取其他数据（包括来自CMDB / CMMS的资产清单数据、设备通信摘要（例如，原始NetFlowdata）、Active Directory数据、移动设备管理（MDM）数据和漏洞管理数据）的能力对于数据关联和分析至关重要。 通常，那些第三方工具是通过API集成的。 此外，我们的内置设备数据交换（DDX）工具使架构映射变得灵活且容易，客户可以将定制的设备属性提取到Ordr平台。

整个组织监控

Ordr认为需要发现和分析组织中的每个连接设备。 例如，在一家医疗保健组织中，IT和设施设备与医疗设备一样脆弱。 连网的发电设备中的漏洞是业务连续性的巨大风险。 MRI中的漏洞可能与未打补丁的医疗工作站一样严重。 一旦您对整个设施中已连接设备的整体情况具有清晰的可见性和丰富的设备上下文，则您将获得足够的信息来提出适当的风险缓解计划和措施。 如果您仅关注设备发现的一个领域，则完全看不到其他风险，这可能会使整个工厂的运营下降。 系统可以合理地对企业中的各种设备，不仅是医疗设备，进行合理分类的唯一方法是必须使用AI / ML之类的现代技术，而不仅仅是依靠DPI的属性。

Ordr继续与众多的客户合作，以改善我们的平台和知识库，了解更专有和特定的设备协议，根据我们每天处理的海量数据训练AI / ML模型，并提高我们的设备分类技术的准确性和精细度，因为 我们确信这将帮助客户从根本上改变其业务以及设施的保护能力。

关于Ordr

Ordr可以轻松保护从传统IT设备到更新且更脆弱的IoT，IoMT和OT的所有连接设备。 Ordr Systems Control Engine使用深度数据包检测和高级机器学习来发现每个设备，分析其风险和行为，映射所有通信并通过自动化策略对其进行保护。全球客户信任Ordr提供实时资产清单，解决风险和合规性并加速IT计划。 Ordr得到包括Battery Ventures，Wing和TenEleven Ventures在内的顶级投资者的支持。 欲获得更多信息，访问www.ordr.net并在Twitter和LinkedIn上关注Ordr 。