

Qosmos ixEngine®

下一代深度数据包检查 (DPI) , 可最大程度地显示流量情况

提供DPI软件的电信、网络和安全供应商中, 过70%选择Qosmos ixEngine在其产品中嵌入第二层到第七层流分类和元数据提取。

关键信息

- ▶ 嵌入到应用程序中的C库
- ▶ 3400个协议插件(包括物联网/SCADA和加密货币), 持续支持和更新
- ▶ 提取5400个应用程序元数据
- ▶ 基于流模式匹配、流预测、双向流关联、行为分析、统计分等的; 协议和应用程序分类
- ▶ 高识别率: 识别OSI模型中2到7层的能力
- ▶ 用于进一步分析和更容易集成的可选库
 - 深度文件检查库
 - 规则引擎SDK
 - GTP库
- ▶ 标准DPI以外的其他功能
 - 加密和规避流量分类
 - 第一包分类
 - 自定义签名
 - 高效化DPI
 - 交易化DPI
 - 自动化DPI
- ▶ 支持服务中软件升级 (又名热插拔) 的常用协议插件版本, 以适应IP流量快速变化的本质
- ▶ 支持DPI引擎的多个实例
- ▶ 模块化架构带来灵活性 (单独的流管理、DPI框架、协议插件和可选模块)
- ▶ 在最新的x86架构上, 每个内核高达10 Gbps *

Qosmos ixEngine 是DPI库,适合希望将详细的实时可见性嵌入其网络或安全产品的软件开发人员。

尽管某些技术仅限于识别IP流背后的应用程序,但Qosmos ixEngine进一步提取了深度,高保真协议和应用程序元数据。

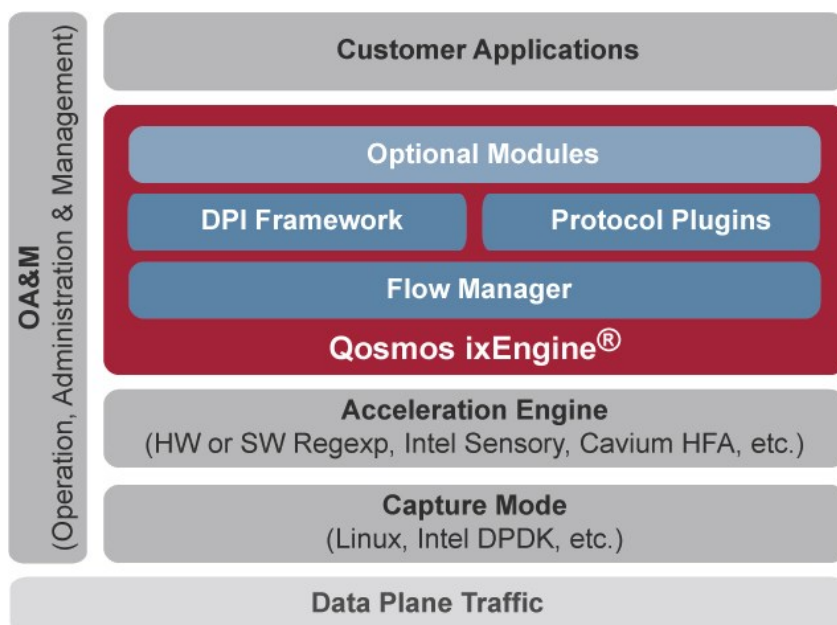
这使开发人员能够在其解决方案中注入应用程序级别的见解, 以全面实时地了解网络流量 (包括加密和逃避流量), 并获得对网络事务和用户行为的详细了解。

我们还提供了一系列可选模块, 用以缩短开发周期。

这些模块 (例如规则引擎或深度文件检查功能) 使用来自分类和元数据提取的输出数据, 并应用进一步的处理, 否则这些处理必须在最终应用程序中构建。

Qosmos ixEngine 专为开发人员而设计,可加快产品开发周期。

即用型软件库和模块减少了与内部开发和维护高度复杂的技术相关的成本和风险。



*性能可能会随着流量模式和网络环境的变化而显著变化。请联系您当地的代表以获取每种情况的详细信息。

超越IP流量分类：元数据提取

Qosmos ixEngine®提取基于网络的应用程序元数据和计算出的元数据的**8个主要类别**：

- ▶ **流量**：例如，每个应用程序和每个用户的流量
- ▶ **服务识别**：例如，VoIP和IM协议及应用程序的服务分类，甚至在加密流中
- ▶ **应用程序用法**：例如，SMB：版本，user_agent长度（用于熵），文件散列
- ▶ **应用程序性能**：例如，VoIP MOS和RFactor之类的计算元数据
- ▶ **标识符**：例如，电子邮件发件人/收件人地址或任何其他可用于实施严格的安全规则的ID
- ▶ **内容**：例如，电子邮件中的链接检测和提取；电子邮件中的附件，可以定向到特定的处理程序，例如第三方防病毒或内容检查
- ▶ **文件元数据**：例如，文件扩展名、大小、类型、名称、内容等，这对于DLP或高级恶意软件检测等用例非常有用
- ▶ **与安全相关的元数据**：例如，在诸如DNS或ICMP之类的协议上进行隧道传输；JA3 / JA3S；NTLM和KRB5相关的元数据

最新的协议插件和元数据

无预先通知地发生在应用程序及其协议之间的不断变化。Qosmos ixEngine提供了更安全的途径来获得可靠，始终最新的DPI技术。Qosmos Labs的专家不断收到有关协议和应用程序更改的信息，并相应地更新插件。更新可即时部署，而不会中断服务。

汇总和计算元数据的扩展

Qosmos ixEngine具有许多扩展，旨在通过提取应用程序元数据来简化操作。扩展可以将流关联以进行继承（信号和用户平面合并），并计算KPI（例如VoIP流的MOS）。

可选库及其他功能

这些库和特殊功能提供了分类数据和元数据的额外处理，以更好地适应一些用例：

- ▶ **自定义签名模块**，可通过用户定义的签名来补充Qosmos签名，以实现专有协议或扩展
- ▶ **深度文件检查**，用于检测文件类型，MIME类型和文件扩展名之间的一致性检查，文件哈希计算以及元数据提取
- ▶ **规则引擎**，用于在运行时执行客户定义的规则（关联，聚合等）
- ▶ **交易化DPI**，以获取特定应用程序内的用户交易作为元数据（例如，在Facebook上下载图片）
- ▶ **自动化DPI**，使用自动化算法对以前未知的流量进行分类
- ▶ **加密和逃避的流量分类**，以跟上公共和专用网络上加密技术的兴起，并识别异常或非法使用流量掩盖应用

高性能和吞吐量

Qosmos ixEngine具有内置的多核支持功能。该软件在Intel架构上通常每个核心处理高达10 Gbps *的流量。

- ▶ 优化的多线程支持，可扩展多达96个内核
- ▶ 在繁重的元数据提取负载下实现高性能
- ▶ 针对业界最高性能的多核处理器的优化代码
- ▶ 利用硬件加速

架构与整合方案

Qosmos ixEngine为嵌入式软件开发人员提供了最简单的L2-L7流分析方法。Qosmos ixEngine的即用型库减少了开发周期、成本和风险，并使开发人员可以依靠Enea旗下Qosmos部门在协议、应用程序和元数据提取领域的专业知识来专注于构建完整的解决方案：

- ▶ 与数据包处理中间件（例如Intel DPDK）的**优化集成**
- ▶ **加速和卸载**配置选项，可与自定义流管理器实现最佳集成
- ▶ **独立的核心解码框架**和协议插件库，可转换为快速流签名更新，同时保持引擎稳定性。协议插件可热插拔
- ▶ **可交换IP碎片整理和TCP流程**重组过程，可用于数据包重新排序
- ▶ **第一个数据包处理**选项，可在用例（例如SD-WAN）中实现最佳流量控制
- ▶ **可选的数据包预过滤**：根据应用要求，Qosmos ixEngine可以解析所有数据包或仅部分数据包
- ▶ **独特且高度可配置的流管理器架构**它可以处理标准，隧道和多路复用流，同时允许不同的内存分配模式以最大的灵活性
- ▶ **支持Qosmos ixEngine的多个实例，以实现最大的实现灵活性**
为了加速集成并确保您利用我们技术的所有功能，Enea提供专业服务并提供访问专家开发人员网络的权限。

支持的操作系统和芯片组

- ▶ Intel x86 (Linux, Solaris, FreeBSD, MacOS, Windows)
- ▶ Cavium Octeon (SE, Linux)
- ▶ Broadcom XLP (Linux)
- ▶ PowerPC (Linux)
- ▶ Tilera Gx (Linux)
- ▶ ARM (Linux)

了解更多

请访问<https://protobook.qosmos.com>找到Qosmos技术认可的协议的完整列表，或在www.qosmos.com/about-us/contact-us/上请求免费的产品评估。