火绒安全携手OpenVINO™工具套件共筑软硬件协同安全新格局

背景

在现代网络环境中，网络安全面临着日益复杂的挑战，包括新兴的勒索软件、多变的木马病毒以及其他先进的持续威胁。这些威胁不断演变，要求安全解决方案不仅要快速反应，还要能在前所未有的规模上进行精确识别和拦截。

针对日益增多的各类恶意程序的网络攻击，火绒安全建立了多层次主动防御系统来有效应对，在病毒检测方面，基于传统模式匹配和行为分析技术已取得了一定的成效。然而，随着恶意软件技术的快速进步，传统方法面临着速度慢、误报率高和适应新威胁的能力不足的问题。为了应对这些挑战，火绒安全采用了基于深度学习的算法来增强其病毒检测能力以及检测效率。这种方法的优点在于其能够持续学习和适应新出现的恶意行为，大大提高了检测的精确度和速度。

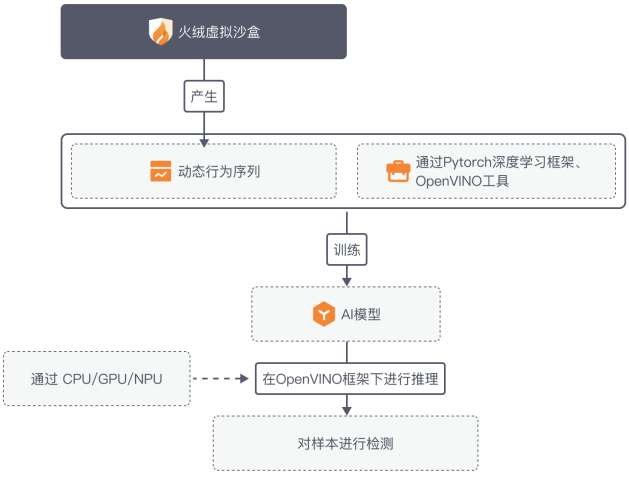
OpenVINO™是英特尔推出的针对深度学习模型进行优化、推理加速以及快速部署的开源工具套件。利用OpenVINO™工具套件，针对病毒检测深度学习模型，火绒安全能够实现

- 模型的优化与推理加速。OpenVINO™提供了一系列的模型优化工具，可以有效减小模型尺寸并加快推理速度，从而更有效地在用户端实现实时威胁检测。
- 模型跨平台的快速部署，以及推理负载的轻松切换。通过OpenVINO™具有的“一次编写，任意部署”的特点，火绒安全的病毒检测深度学习模型可以很方便地部署在多个硬件设备上，并可以在不同的设备上快速地进行推理负载的切换。通过利用英特尔酷睿Ultra平台中的神经处理单元（NPU），火绒安全可以将计算密集型的病毒扫描任务迁移到这些专用硬件上。这不仅减轻了主CPU的负担，还降低了整体系统的功耗，同时保持了扫描任务的高效率和低延迟。
- 更快速更省力的软件开发。目前，OpenVINO™已经同时支持英特尔®架构以及ARM架构的CPU作为运行深度学习模型推理的硬件，同时，也支持英特尔的集成显卡、独立显卡、以及NPU、FPGA上的模型部署。由于这种跨平台多架构硬件设备的支持，火绒安全也可以利用OpenVINO™缩短病毒扫描监测软件在跨平台上的开发时间，同时大大减少了开发的工作量。

火绒安全携手OpenVINO™工具套件以及英特尔新一代酷睿Ultra处理器，这种软硬件协同的方法不仅提高了终端安全的效率，也为用户创造了更为安全和高效的计算环境。

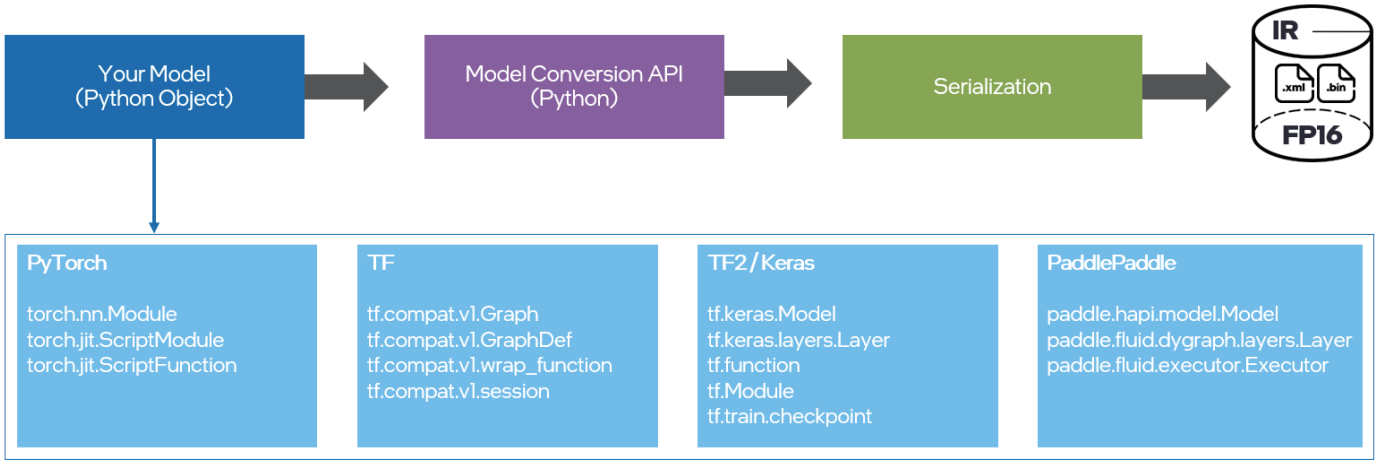
基于OpenVINO™的病毒扫描监测模型的优化与推理加速

为了应对恶意软件和病毒技术快速进步带来的挑战，火绒安全采用了基于深度学习的算法来增强其病毒检测能力以及检测效率，流程图如下图所示。



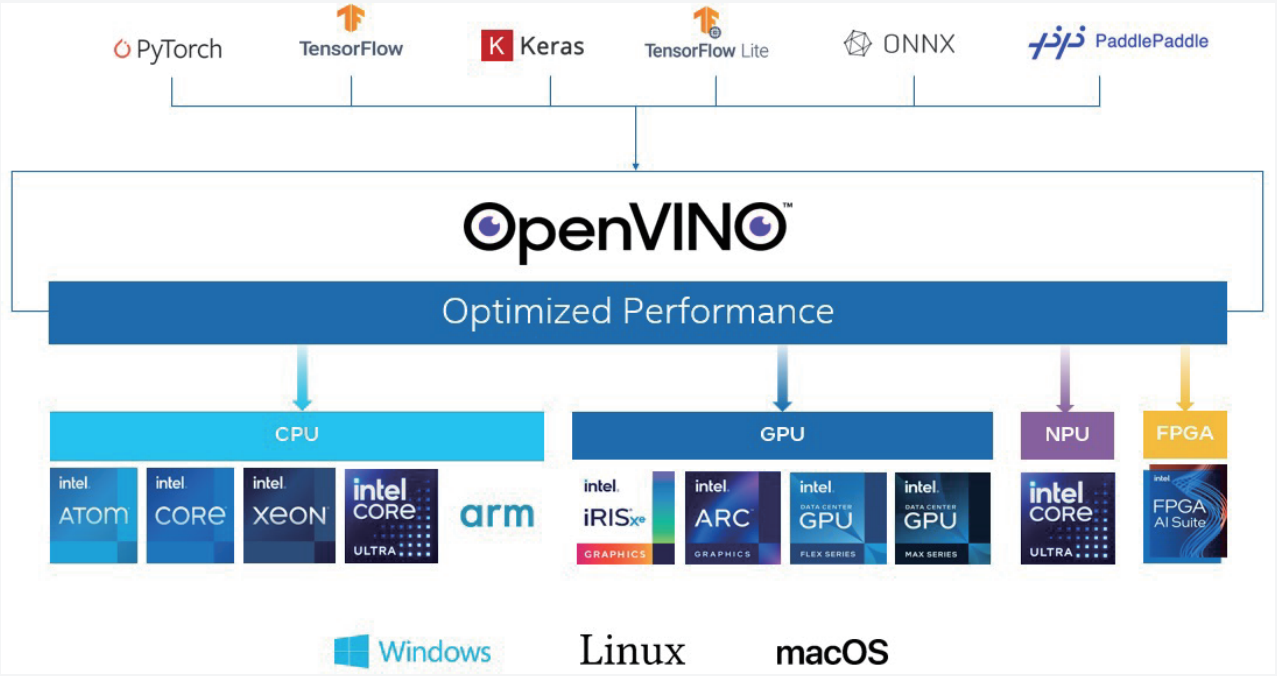
利用虚拟沙盒中进行病毒扫描而收集到的动态行为序列组成的数据集，火绒安全基于PyTorch深度学习框架进行模型训练，并获得了可高效高准确度进行病毒检测的AI模型。接着，火绒安全利用OpenVINO™工具套件，实现了模型优化、并将该模型根据不同用户使用的硬件平台进行简单快速的部署。

首先，利用OpenVINO™提供的模型优化工具，例如模型转换工具、神经网络压缩框架（NNCF）等，火绒安全可以将训练好的病毒扫描监测模型由原始的PyTorch模型格式转化为OpenVINO 中间表达格式（IR格式），实现对模型的优化压缩。经OpenVINO™模型转换与优化压缩后，相对于PyTorch以及ONNX的模型格式，模型占用体积可以减小50%左右。由此，模型在运行推理时的推理速度也可以提到显著提升，提升幅度达到20%以上。使得火绒安全的病毒检测算法能够实现更快的响应时间和更高效的运行，显著提升病毒的检出速度和准确度。



基于OpenVINO™的病毒扫描监测模型快速部署

OpenVINO™的另一个重要特点是其支持跨平台的模型部署能力，无需重写大量代码，可以实现深度学习模型的无缝迁移，达到“一次编写，任意部署”，这对于快速响应新出现的网络威胁尤为重要。特别是针对新一代酷睿Ultra处理器中的NPU（神经处理单元）的支持。这使得火绒安全可以轻松将优化后的深度学习模型部署到各种硬件平台上，包括但不限于英特尔和ARM架构的CPU以及英特尔的GPU。自OpenVINO™ 2024.0的版本开始，深度学习模型可以很方便的部署在英特尔酷睿Ultra平台中的NPU上。由于NPU具有低功耗的特点，火绒安全的深度学习模型可以在NPU上持续进行病毒的扫描和监测、且保持较低的耗电量，为搭载了酷睿Ultra的用户设备提供较高的能效利用率。同时，将深度学习模型推理迁移到NPU上，也很好地释放了CPU上的工作负载，使得CPU的占用率在病毒持续扫描监测时仍然保持较低的水平，从而使得用户对病毒扫描无感、对其它的工作负载不会造成影响。



异构架构支持，开发省时省力

OpenVINO支持包括英特尔X86和ARM在内的多种CPU架构，这为开发人员提供了极大的灵活性和便利。异构架构的支持意味着开发者可以编写一次代码，然后将其部署到多种硬件平台上，无论是在个人电脑、服务器还是移动设备上。这种能力不仅简化了开发流程，也使得火绒安全可以轻松适应各种硬件环境，保证软件的广泛兼容性和高效性。此外，这种支持也使得火绒安全能够更好地利用不同设备的特定硬件加速功能，进一步提高其产品的性能和效率。

展望未来，火绒安全计划继续深化与英特尔的技术合作，通过不断的技术研发和创新，旨在为用户提供更为高效、智能的安全解决方案。随着AI技术的不断进步和应用的深化，火绒安全与包括OpenVINO™工具套件、酷睿Ultra处理器在内的英特尔软硬件技术的合作不仅提升了病毒扫描的效率，还为终端用户提供了一个更加安全、快速且能效优越的解决方案。

关于火绒安全

火绒安全成立于2011年9月，是一家专注、纯粹的安全公司，致力于在终端安全领域，为用户提供专业的产品和专注的服务，产品功能涵盖“恶意代码防护”、“系统防护”、“网络防护”、“身份鉴别”、“资产管控”、“入侵防范”等，并持续对外赋能反病毒引擎等相关自主研发技术。

关于英特尔

英特尔(NASDAQ:INTC)作为行业引领者，创造改变世界的技术，推动全球进步并让生活丰富多彩。在摩尔定律的启迪下，我们不断致力于推进半导体设计与制造，帮助我们的客户应对最重大的挑战。通过将智能融入云、网络、边缘和各种计算设备，我们释放数据潜能，助力商业和社会变得更美好。如需了解英特尔创新的更多信息，请访问英特尔中国新闻中心 newsroom.intel.cn 以及官方网站 intel.cn。

intel

火绒安全
www.huorong.cn

实际性能受使用情况、配置和其他因素的差异影响。更多信息请见 www.Intel.com/PerformanceIndex

性能测试结果基于配置信息中显示的日期进行测试，且可能并未反映所有公开可用的安全更新。详情请参阅配置信息披露。没有任何产品或组件是绝对安全的。

具体成本和结果可能不同。

英特尔技术可能需要启用硬件、软件或激活服务。

英特尔未做出任何明示和默示的保证，包括但不限于，关于适销性、适合特定目的及不侵权的默示保证，以及在履约过程、交易过程或贸易惯例中引起的任何保证。

英特尔并不控制或审计第三方数据。请您审查该内容，咨询其他来源，并确认提及数据是否准确。