SOPHOS
Security made simple.

Intercept X Deep Learning深度学习

Intercept X 将深度学习与同类最佳的防漏洞利用攻击技术、CyptoGuard 防勒索软件、根本原因分析等相结合，打造业内最全面的端点保护解决方案。独特的功能组合使得 Intercept X 能够阻止最广泛的端点威胁。

产品亮点

- 首屈一指的恶意软件侦测引擎
- 阻止已知和前所未见的恶意软件
- 先发制人在恶意软件执行前加以阻止
- 不依赖特征码
- 即使主机离线也可提供保护
- 在约 20 毫秒内侦测恶意软件
- 历经数以亿计样本的训练
- 2016 年 8 月获得 VirusTotal 认可
- 将文件分类为恶意、潜在不需要应用程序 (PUA) 或良性
- 无需任何额外培训即可使用
- 占用空间极小（不到 20MB）
- 专注于 Windows 可移植可执行文件

现在大多数的安全产品都是被动应对的，而且应对速度过慢。随着端点攻击数量和复杂程度的不断增加，传统方法已经难以跟上脚步。例如，SophosLabs 每天分析超过 400,000 个新恶意软件样本。更甚的是，SophosLabs 发现 75% 的恶意软件对于某一个企业来说是独特的，这使得挑战更加艰巨。

深度学习作为机器学习的高级形式，有助于改变我们对待端点安全的方式，而 Intercept X 正在引领这一变革。集成深度学习的 Intercept X 将端点安全方法从被动应对变为主动预防未知威胁。

深度学习与其他类型机器学习的对比

> “Intercept X 采用类似人脑的深度学习神经网络……这样会提高现有和零日恶意软件侦测率，减低误报率。”
>
> ESG Lab Report，2017 年 12 月

许多产品号称采用机器学习，但不是所有机器学习都是一样的；Sophos 采用深度学习侦测恶意软件。深度学习以人脑的工作方式为灵感运作，也称为“深度学习神经网络”或“神经网络”；这跟经常用于面部识别、自然语言处理、自动驾驶汽车，以及其他计算机科学及研究的尖端领域所采用的机器学习为同一种。

深度学习的性能一直超越其他机器学习模型，包括随机树、k-均值聚类或 Bayesian 网络，但需要海量数据和计算能力才能建立起有效模型。Sophos 利用 SophosLabs 在过去 30 年大量的恶意软件收集和分析工作，以及每天从 1 亿个以上的端点收集的数据，实现这一强大模型。

相比端点安全常用的其他类型的机器学习，深度学习具有一些先天的优点：

更智能：深度学习模型通过多个分析层处理数据，就像人脑的神经元，每一层显著提高模型的性能。它分析不同输入特征之间的复杂关系，自动发现输入数据的最佳组合和操纵，而这是人类无法断定的领域。这意味着 Sophos 深度学习恶意软件检测模型将能够侦测到其他机器学习引擎注意不到的恶意软件。

更灵活扩展性：深度学习能够轻松扩展至数以亿计的训练样本，考虑到 SophosLabs 每周分析 280 万个新恶意软件样本，这一点很重要。由于可以不断吸收海量训练数据，我们的模型可以将整个可观察到的威胁态势“记忆”起来，为训练过程的一部分。通过处

理更多的输入数据，深度学习可以更准确预测当前威胁，同时始终保持最新。

更轻盈：传统机器学习方法造成模型体积庞大，有时候可占用数 Gb 磁盘空间；而 Sophos 深度学习方法实现高度压缩模型。Sophos 深度学习模型体积极为细小，在端点上占用不到 20MB 空间，几乎不影响性能。

Sophos 深度学习功能

Sophos 提供深度学习专业知识和业内性能最高的恶意软件侦测引擎：

经验丰富：和竞争对手不同，我们长期以来一直是网络安全机器学习领域的专家，在生产环境部署恶意软件侦测深度学习模型多年。Sophos 恶意软件侦测模型由我们的数据科学家团队采用 DARPA 驱动技术创建。2010 年，美国国防部高级研究计划局（US Defense Advanced Research Projects Agency，DARPA）创建网络基因计划 (Cyber Genome Program)，用于发现恶意软件和其他网络威胁的“DNA”；这正是搭载在 Intercept X 上算法的起源。

备受认可：我们的模型一直保持开放透明，除了在 Black Hat 等行业会议上展示我们方法的详细信息，我们也并不避讳独立第三方测试我们的软件。2016 年 8 月这模型获得 VirusTotal 认可，并且一直在 NSS Labs 等第三方测试机构处获得高评分。在所有方面，模型都证明极为有效，同时误报率低。

> “我们测试过的最佳性能分数之一”
>
> Maik Morgenstern，AV-TEST 首席技术官

性能：卓越</9Sophos 深度学习技术速度极快。短短 20 毫秒，模型就能从一个文件中提取数百万个特征，进行深度分析，从而断定文件是良性还是恶性。整个过程在文件执行前经已进行。

SophosLabs：用于训练的数据是任何模型最重要的因素之一。我们的数据科学家团队隶属于 SophosLabs 小组，能够访问数以亿计的样本，这使得他们能够在模型中做出最佳预测。两个小组的融合还是实现了更好的数据标签（进而实现更好的建模）。数据科学家和网络威胁分析人员团队之间关于威胁情报和现实反馈的双向分享，不断提高模型的准确度。

> “Intercept X 阻止到我们遇到的所有复杂高级攻击”
>
> ESG Lab Report，2017 年 12 月

立即免费试用

注册 30 天免费评估版
sophos.com/zh-cn/interceptx

中国销售 (北京)
电话: 400 650 6598
电子邮件: salescn@sophos.com

中国销售 (上海)
电话: +86 21 3251 7160
电子邮件: salescn@sophos.com

中国销售 (广州)
电话: +86 136 0241 6506
电子邮件: salescn@sophos.com

18-01-02 DS ZHCN (2897-DD)

SOPHOS