解决方案简介

FortiAI Virtual Security Analyst™

让安全运营团队摆脱重负，反守为攻

管理层摘要

由于威胁数量、速度和复杂性不断增加，各行企业安全运营团队已经变得不堪重负。幸运的是，为了减轻他们的负担，安全架构师正在尝试一种新工具 — 新一代人工智能 (AI)。作为将 AI 应用于网络安全领域的先驱者，Fortinet 推出了 FortiAI 虚拟安全分析师(Virtual Security Analyst™)来解决这些挑战。这款 FortiAI 是最新 AI 驱动型威胁防护技术，可在不到一秒内完成攻击者对网络渗透的威胁分析，从而让安全团队有机会抢在黑客入侵网络之前阻止恶意软件和攻击。

61% 的企业表示，现今如果没有 AI 技术的帮助，他们就无法检测潜在威胁。[1]

随着高级威胁形势的不断演变，四面楚歌的安全运营团队已经几近崩溃，看不到一丝缓解的希望。威胁数量、速度和复杂性的极速攀升让安全架构师开始纷纷寻求新的出路。由于告警数量不断增加，42% 的组织因告警数量太多而忽略了很多告警。[2] 许多组织也无力增加人手。此外，网络安全技能型人才短缺问题甚至将进一步恶化，目前这一缺口已增加到超过 400 万。[3]

AI 在网络安全领域的演变

网络安全公司几年来一直使用机器学习 (ML) 打击网络罪犯，尤其是在威胁检测领域。训练算法可以通过机器学习增强识别恶意文件特征的准确性，从而实时检测包括零日攻击在内的高级威胁。[4] 这一不断发展的安全技术是当今组织的必备法宝。例如，最近一项研究发现，如果没有它的帮助，60% 的组织将检测不到重大威胁。[5]

但是单凭更好的威胁检测并不能解除安全运营团队的负担，更何况检测升级意味着需要手动处理的警报数量也将加大。因此，企业还需要提高自动化水平，尤其是在威胁响应和安全策略领域。幸运的是，新一代 AI 有望让安全运营团队减轻压力，同时提高整体工作效率。

新一代 AI：深度神经网络

为方便说明新一代 AI 在网络安全方面的潜力，我们先来解释一些术语的含义（图 1）：

- **AI** 是一个笼统的术语，指机器模仿人类行为的能力。
- **ML** 是 AI 的一个分支，它使用数据来解决线性问题，比如进行预测或执行任务。人工神经网络 (ANN) 是一种常见的 ML 方法。人工神经网络使用软硬件来建立一种通过 ML 训练模拟人脑神经元运行机制的配置。模型将会源源不断地获得大量信息，然后系统对这些信息进行分析，并根据恶意软件或攻击媒介采用的新策略和具备的功能调整算法。
- 深度神经网络（DNN，有时又称为深度学习）是一种 ML 技术，它使用多个 ANN（输入和输出层之间具有两层或更多层）对复杂的非线性关系进行建模。

为了理解标准 ML 和 DNN 的不同，我们来看一个例子。标准 ML 可用于向计算机教授英语字母以及如何通过排列字母构成单词，从而最终提供一个含定义和图片的英语单词词典。借助 ML，计算机可以识别在数据集中找到的任何单词的含义，比如蜜蜂、授粉、花朵、田野和白天等。而 DNN 可以训练计算机根据过去呈现的每个特征的图像，描述蜜蜂白天在田野里给花朵授粉的新照片。

计算机通过 DNN 实现的这种理解和分析可让 AI 在网络安全领域获得突破性的应用。当 AI 仅用于威胁检测时，它可能会让安全运营团队的压力不降反增，因为它只会为数量本就庞大的告警雪上加霜，并增加威胁没有得到及时响应的可能性。

但是，如果使用 AI 进行有关威胁响应的智能决策，甚至提供有关安全策略的实用洞察，安全运营专家的困境就会峰回路转。这些专家或工程师可以节省宝贵的时间来继续专心实施安全策略，同时将多数威胁响应工作留给虚拟安全分析师来实时自动化处理

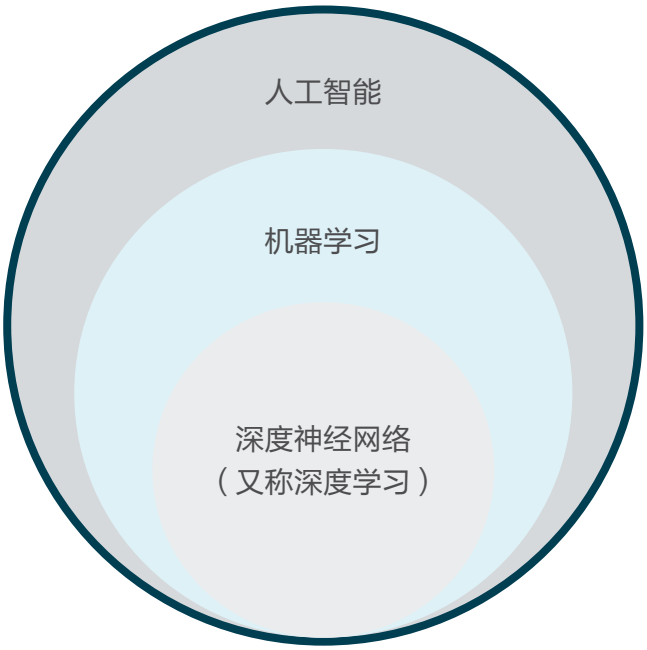

图 1：AI、ML 和 DNN 之间的关系。

八年 AI 技术积淀

Fortinet 是最先将 AI 用于威胁检测的拓荒者之一，在历经四年的运算训练后，于 2012 年推出了基于 ANN 的自演进式检测系统 (SEDS)。SEDS 每天分析数百万个对象，并查验哪些对象是恶意的。然后，它将这些信息推送到 Fortinet Security Fabric 产品中。

现在，这个由 FortiGuard 实验室管理的 SEDS 已使用有监督和无监督 ML 进行了共 12 年的训练，能够根据威胁特征极其准确地实时检测未知和多态威胁，且误报率几乎为零。此后，Fortinet 为 FortiWeb Web 应用防火墙 (WAF) 添加了在线 Web 流量应用分析功能，在 FortiSandbox 中引入了基于 AI 的分析，并将基于 AI 的用户和实体行为分析 (UEBA) 添加到 FortiInsight 和 FortiEDR 基于 AI 的高级终端安全模块中。

“ 知己知彼，百战不殆。‘实时响应可以加大您击退对手的成功几率’。”[6]

FortiAI 虚拟安全分析师（VSA）：新一代本地 AI

Fortinet 是目前第一家提供基于 DNN 技术的本地虚拟安全分析师的公司。FortiAI 虚拟安全分析师 堪称 Fortinet SEDS 2.0，是业内首个在本地嵌入独立自演进式 AI 以模仿信息安全分析师工作职能的产品。它与人类安全分析师一样，能够适应新的攻击并获得日积月累的经验。但与之不同的是，它以机器的速度执行操作。它使用 DNN 自动执行事件调查，创建量身定制的威胁情报，并以机器速度中断针对性攻击。

基于 FortiAI DNN 的无监督学习模型可以说是当之无愧的“ 友好型人工智能 ”(FortiAI) —— 一个业内梦寐以求的目标。借助那些通过 ML 实现的功能，虚拟安全分析师能够以日益增进的速度和准确性识别和分析威胁事件，而不只是单次攻击的检测，进而提高安全人员的“ 价值 ”和工作效率。

使用 AI 了解针对特定组织的攻击

为了以机器速度获取威胁情报，同时赶上高级威胁形势的演进步伐，FortiAI 会日积月累地学习并适应针对特定组织的新攻击，从而不断改善和优化威胁防护生命周期。FortiAI 能够识别和分析无文件和基于文件的恶意软件，并在不到一秒内准确无误地确定整个组织内受感染的系统，以及之间的感染 / 传播关系链。

为此，FortiAI 使用 DNN 技术做出本应由安全分析员手动调查攻击才能进行的决策，包括：

- **对攻击进行自定义分类**，比如勒索软件、加密劫持、蠕虫、后门攻击、数据泄漏、僵尸网络和 Rootkit
- **调查攻击源**，使用时间戳跟踪感染源，提供从无到有的整个横向扩散感染过程的全面可见性
- **恶意软件分析**，通过 FortiAI DNN 观察到的特征确定恶意软件的类型，并提供每个感染事件的时间线。用科学术语来说，这类似于微型杀伤链模型，整个威胁的展开过程（包括所采用的技术）一目了然。例如，“ 时间 0”：下载 HTML 文件；“ 时间 1”：在浏览器中利用恶意代码；“ 时间 2”：将木马下载到用户本地或临时目录。FortiAI 预载了 30 亿个恶意软件特征，并且会随着时间的推移不断增添。

当 FortiAI 虚拟安全分析师 执行这些分析时，其全面集成的 FortiGate 下一代防火墙 (NGFW) 可以拦截识别出的威胁。然后，安全运营人员再根据威胁情报实施全网安全控制。

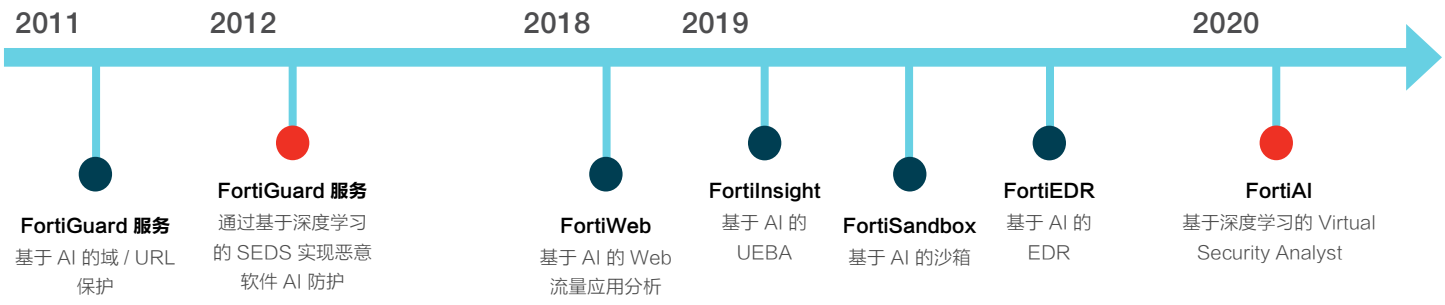

图 2：Fortinet AI 和 ML 应用时间线。

FortiAI 对网络安全团队的好处

FortiAI 虚拟安全分析师 可以帮助安全专业人员摆脱重负、反守为攻，同时提高运营效率。它具有以下主要优势：

1. 加速抵御攻击。通过对每个安全事件进行实时自动化调查，安全人员可以更快地响应以机器速度发起进攻的自动化威胁。拖得越久，入侵的影响就越大，因此实时响应是将损害最小化的最佳方法。
2. 缩短威胁暴露时间窗口。实时分析可帮助组织在等待厂商开发应用补丁或反恶意软件签名时增强抵御能力。而且，系统可以在不到一秒钟的时间内发出警报，然后安全运营团队可通过“ 虚拟补丁 ”阻止恶意软件。
3. 通过真正消除误报提高工作效率。组织不必再将通用威胁源应用到安全控制中，也不必再手动调查每一个误报。[8]

> “ 未来的战场是数字化的天下，而 AI 是无可争议的首选武器。”[7]

[1] "Reinventing Cybersecurity with Artificial Intelligence: A new frontier in digital security," Capgemini, accessed January 27, 2020.

[2] Jon Oltsik, "Dealing with Overwhelming Volumes of Security Alerts," ESG, March 3, 2017.

[3] "(ISC)² Finds the Cybersecurity Workforce Needs to Grow 145% to Close Skills Gap and Better Defend Organizations Worldwide," (ISC)², November 6, 2019.

[4] "Using AI to Address Advanced Threats That Last-Generation Network Security Cannot," Fortinet, June 8, 2019.

[5] "Reinventing Cybersecurity with Artificial Intelligence: A new frontier in digital security," Capgemini, accessed January 27, 2020.

[6] David Strom, "Understanding the Relationship Between AI and Cybersecurity," Security Intelligence, March 22, 2018.

[7] William Dixon and Nicole Eagan, "3 ways AI will change the nature of cyber attacks," World Economic Forum, June 19, 2019.

[8] Chris McDaniels, "Is Threat Intelligence Garbage?" Dark Reading, March 23, 2018.

February 6, 2020 12:54 AM

D:\Fortinet\Solution Briefs\teal solution briefs\FortiAI\sb-fortiai-virtual-security-analyst-V1.2-262020-1254AM

594577-0-0-EN