SOPHOS

需要 EDR 的 5 大理由

端点侦测与响应 (EDR) 工具旨在为端点安全补充更高的侦测、调查和响应功能。但是，围绕 EDR 工具的大肆宣传可能让人难以理解其正确用途和需要的原因。更严重的是，现在的 EDR 解决方案往往难以为多数企业提供价值，因其使用困难，缺乏足够的保护功能，而且资源密集。

Sophos Intercept X with EDR 将智能 EDR 与行业顶尖的端点和服务器保护集成在一个解决方案中，成为企业解决安全事件难题的最轻松方式。下面我们将介绍更多考虑 EDR 解决方案的其他理由。

维持 IT 安全操作卫生，追踪隐秘威胁

不同企业里，IT 操作和 IT 安全人员可能属于同一团队，独立操作，或者甚至是同一个人。无论是何种设置，这两个领域都需要 EDR 工具的不同用例，因此工具应能够执行两组任务，保持可访问而不影响性能。

对于 IT 操作，管理员保持企业资产处于良好状态非常重要。例如，找出存在性能问题的计算机，如磁盘空间低或内存使用量高。找到需要打补丁，存有弱点的程序的设备。跟踪不必要启用 RDP 或仍启用来宾帐户的端点和服务器。Sophos EDR 为管理员提供工具，提出所有这些以及其他问题，通过研究性能问题、安装补丁和禁用 RDP 及来宾帐户，远程访问设备修复安全漏洞。

网络安全专家需要能够追踪其端点防护无法自动解决的狡诈回避的威胁。他们的 EDR 工具需要高效追踪威胁迹象 (IoC)，如：找出尝试连接非标准端口的进程，编辑过文件或注册表项的进程，伪装为其他内容的进程，跟踪单击过网络钓鱼电子邮件链接的员工。Sophos EDR 让企业轻松快速的在整个资产内执行此类调查。然后轻松远程访问需关注的设备，更加深入挖掘，部署鉴证工具和终止可疑进程。

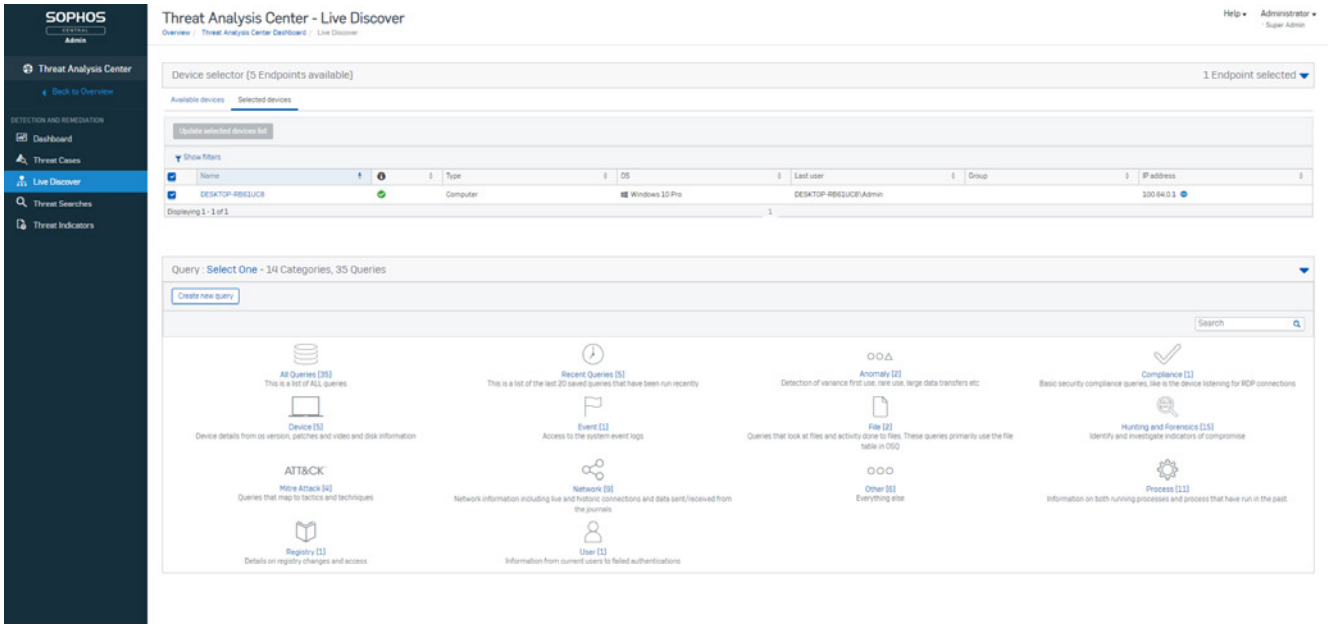

图 1: Sophos Intercept X with EDR 允许用户提出整个资产内的详细问题

侦测未注意到的攻击

在网络安全方面，只要有足够时间和资源，甚至最先进的工具都可以被打败，因此难以真正了解发生攻击的时间。企业通常单纯依赖预防以保持受保护状态，预防很关键，而 EDR 带来另一层侦测功能，有可能发现未注意到的事件。

企业可以利用 EDR 搜索受感染指标 (IOC)，进行侦测攻击，这是一种寻找错过的攻击的快速且直接的方法。威胁搜索通常在接到第三方威胁情报通知后开始：例如，政府机构（如 US-CERT、CERT-UK 或 CERT Australia）可能通知企业其网络中存在可疑活动。这通知会附带 IOC 列表，可以作为断定发生情况的起点。

Intercept X 中的威胁迹象功能提供最重要可疑事件的列表，这样分析师准确了解应调查的内容。利用 SophosLabs 机器学习功能，按威胁分数展示最重要可疑事件列表。这样方便分析师安排工作优先顺序，将精力集中在最重要的事件。

了解在哪里开始后，分析师可以在整个资产内跟踪该可疑项的所有实例，快速采取措施清理。此外，他们可以利用强大的 SQL 查询跟踪其他威胁迹象，如编辑注册表项的进程和尝试连接非标准端口的进程。

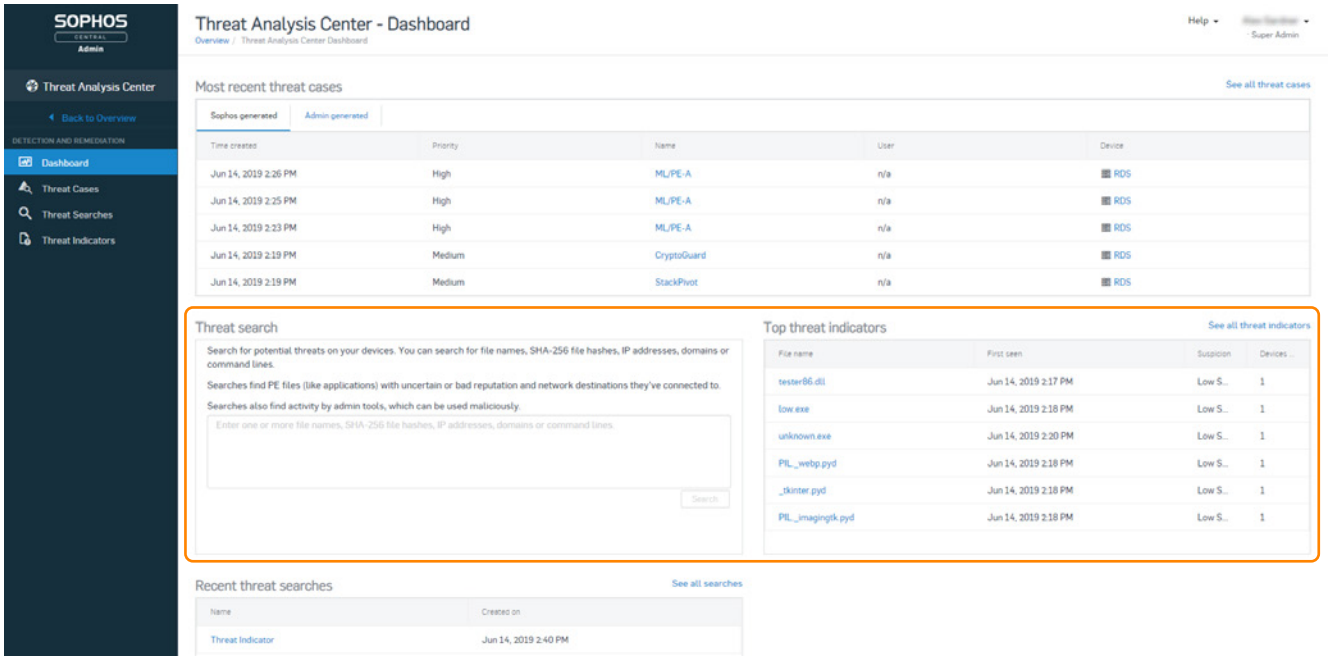

图 2: Sophos Intercept X with EDR 提供搜索网络中威胁迹象的功能。还利用机器学习确定应调查的可疑事件。

提出详细问题和给予在何处开始行动的指导的能力，加上精选的威胁情报，为管理员带来全球最佳功能，使 Sophos EDR 使用直接而不牺牲性能和精细度。

更快速响应潜在事件

侦测到事件后，IT 和安全团队通常尽快将其修复，以减小攻击蔓延的风险和限制任何潜在危害，最关键的问题无疑是如何摆脱每种威胁。安全和 IT 团队平均用 3 个小时以上解决每个事件，EDR 可以显著加快这一过程。

分析师在事件响应过程中的第一步是阻止攻击蔓延。Intercept X with EDR 随需要隔离端点和服务器，这是阻止威胁在环境中扩散的关键步骤。分析师通常在调查前执行此操作，在断定最佳行动方案的同时，争取时间。

调查过程可能缓慢而痛苦，这当然假定调查必定发生。传统上，事件响应重度依赖于高度熟练的分析师人员。大多数 EDR 工具还重度依赖分析师了解要提出的问题和如何解释答案。但是有了 Intercept X with EDR 后，借助引导调查提供建议的下步措施、清晰可见的攻击表示以及内置专业技术，所有技术水平的安全团队都能快速响应安全事件。

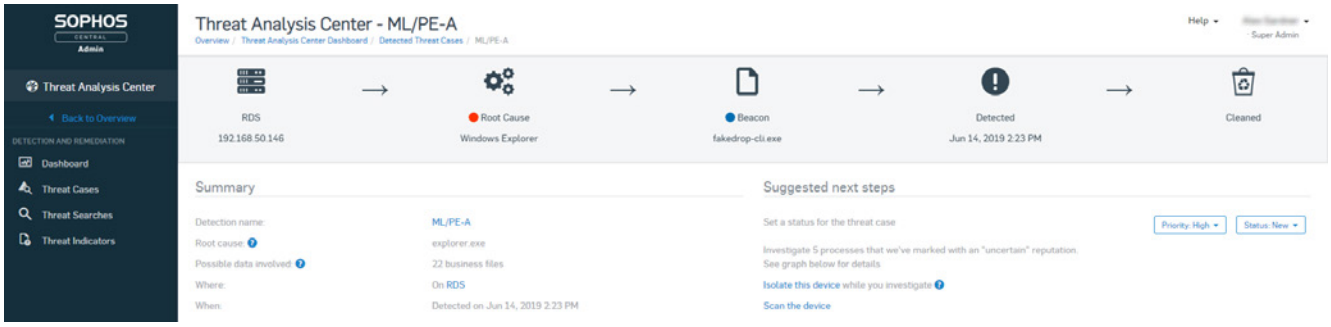

图 3: 引导事件响应提供建议的下步措施和按需端点隔离，快速安全解决事件。

Sophos EDR 还具有通过命令行界面远程访问设备的功能。非常适合快速响应，即使员工不在办事处上班。访问设备时，管理员可以部署鉴证工具执行进一步调查，安装/卸载软件，终止进程和重新启动设备。

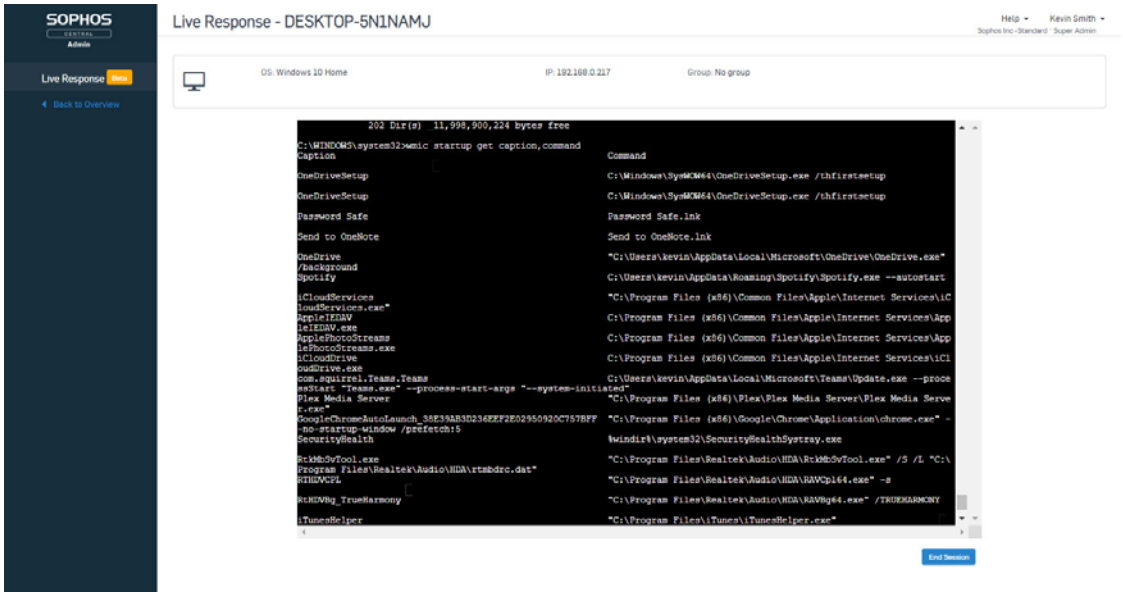

图 4：Intercept X with EDR 中的操作按钮提供多个补救选择，“清理并阻止”是最常用的。

提高专业技术水平而不需增加人手

很多寻求端点侦测和响应功能的企业将“员工知识”列为采纳 EDR的最大障碍。这并不令人奇怪，因为多年来人们一直在讨论人才匮乏，希望找到合格的网络安全专业人才。这一障碍在小型企业中尤为明显。

企业尚未实施 EDR 的主要理由

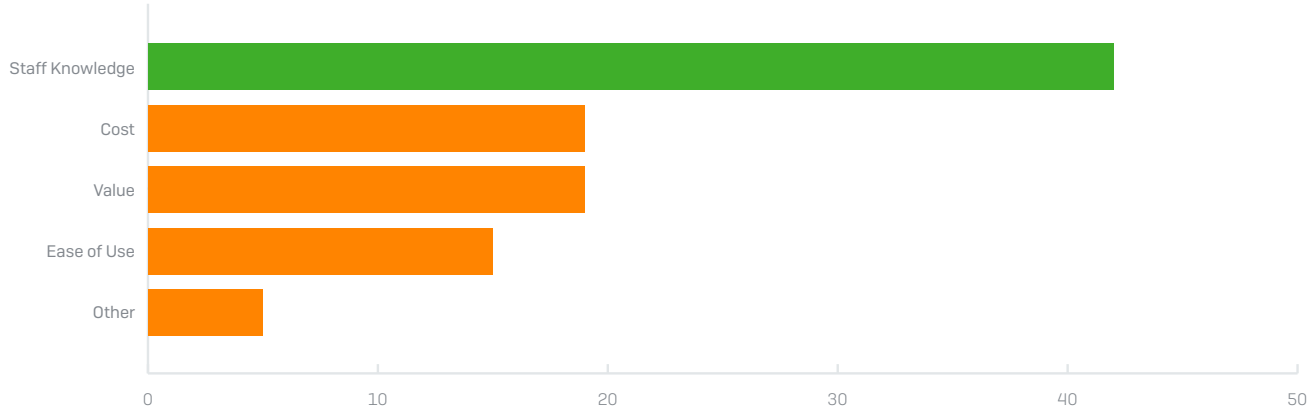

图 5: 员工知识被视为企业尚未采用端点检测与响应 (EDR) 解决方案的重要原因（来源：Sapio 与 Sophos 的合作研究，2018 年 10 月）

为了解决员工知识的不足，Intercept X with EDR 再现了稀缺分析师所具备的功能。它利用机器学习整合深入安全信息，通过 SophosLabs 威胁情报加以强化，这样您无需增加人手即可提高专业知识水平。智能 EDR 功能帮助弥补因缺乏员工知识而带来的不足，代替多界别分析师的功能：

- **安全分析师**：此类前沿分析师的任务是筛选事件，确定需要立刻解决的提醒。他们最好还能够主动侦测任何未注意到的攻击。Intercept X with EDR 自动检测潜在威胁并排定优先顺序。利用机器学习发现可疑事件，并给出威胁分数。具有最高分数的事件最为要紧。分析师可以快速看到需要关注的重点，并开始调查。
- **恶意软件分析师**：企业依赖恶意软件专家，他们擅长反向工程可疑文件以进行分析。这种方法不仅耗时和难以实现，而且大部分企业都不具备这种网络安全成熟度。恶意软件分析师的职责是来确定未被阻止的文件实际是恶意的，他们还考察已确定为恶意但实际是误报的文件。Intercept X with EDR 利用机器学习提供更好的恶意软件分析方法。利用行业最佳的端点恶意软件侦测引擎，恶意软件会被自动进行极其详细的分析，细分到文件属性和代码组件，并与数以百万的其他文件进行比较。分析师很容易看出与“已知安全”和“已知恶意”文件类似的属性和代码段，从而确定应阻止还是允许文件。
- **威胁情报分析师**：调查可能依赖第三方威胁情报（通常需要额外成本）来增加威胁信息和环境。需要分析师来解读并整合这些数据，以确保带来价值。威胁情报可以作为调查的起点，询问安全社区他们认为的可疑文件，或者确定攻击是否针对企业。Intercept X with EDR 访问 SophosLabs 的按需威胁情报，为 IT 和安全管理员提供收集更多信息的能力。为了保持对威胁态势的完全可见性，SophosLabs 每天跟踪、解构并分析 400,000 个独特且以前未发现的独特恶意软件攻击，不断寻找最新最强大的攻击技术。收集、汇总并总结这些威胁情报，进行简单的分析，这样，没有专门威胁情报分析师，或者威胁来源成本高，又在理解威胁情报方面存在困难的团队可以从当今全世界顶级的网络安全研究和数据学团队中获益。

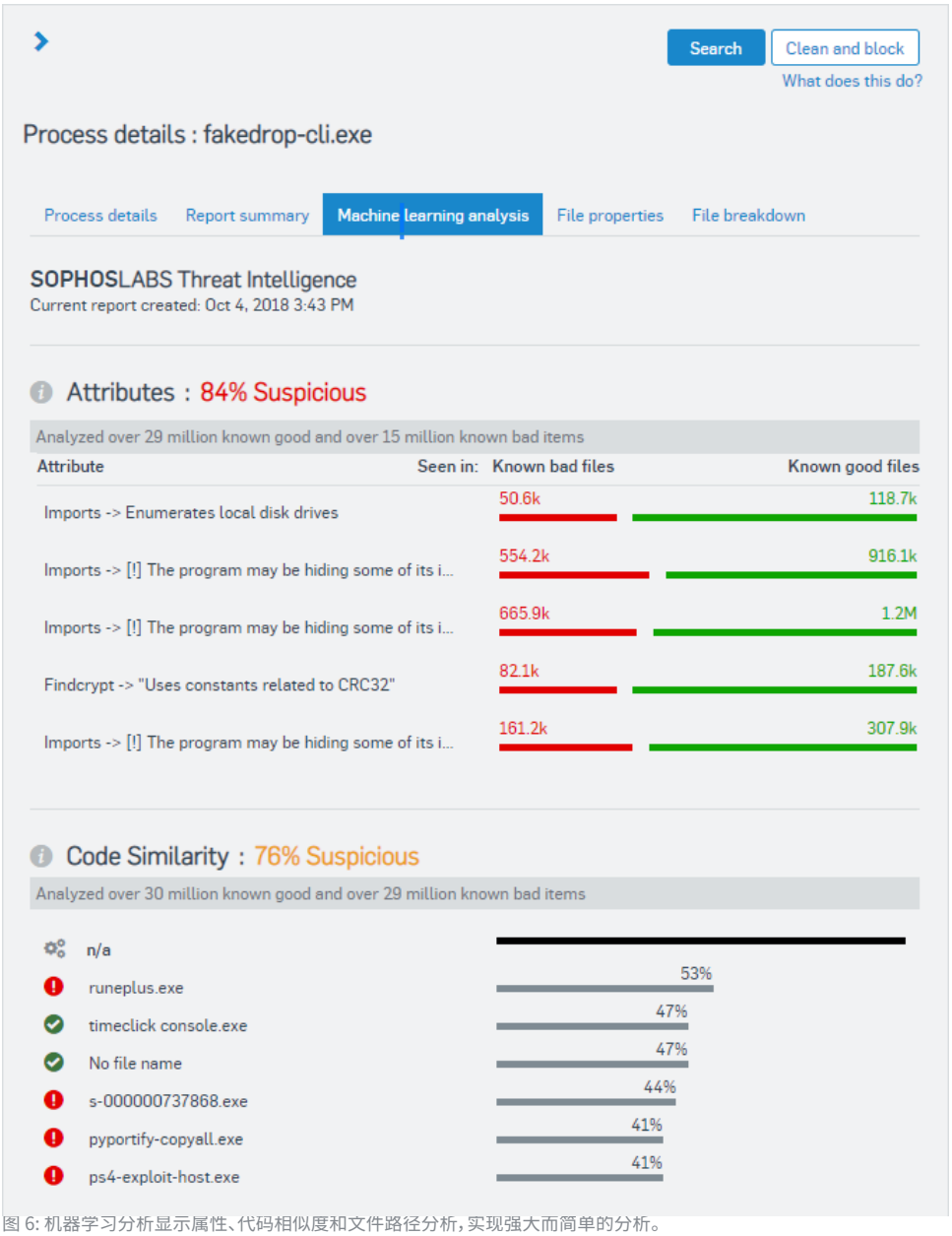

图 6: 机器学习分析显示属性、代码相似度和文件路径分析，实现强大而简单的分析。

Managed Threat Response (MTR)

寻求管理 EDR 的帮助?Sophos 的 MTR 服务融合科技与专家分析，改进威胁追踪和检测，更加深入调查警报，采取针对性操作响应威胁。

了解攻击如何发生，如何阻止其再次发生

安全分析师不断重现遭受攻击的噩梦：执行官咆哮道“这是怎么回事?!”，分析师只能耸耸肩膀表示无奈。找出并移除恶意文件可以解决当前问题，但不能阐明恶意文件最初如何进入，或者关闭攻击前攻击者做了什么。

Intercept X with EDR 附带的威胁事件重演重点指出导致侦测的所有事件，方便理解恶意软件接触了哪些文件、进程和注册表项，以断定攻击的影响范围。它提供整个攻击链的可视化表示，确保自信地报告攻击发起方式和攻击的区域。更重要的是，了解攻击的根本原因后，IT 团队将更有可能阻止其再次发生。

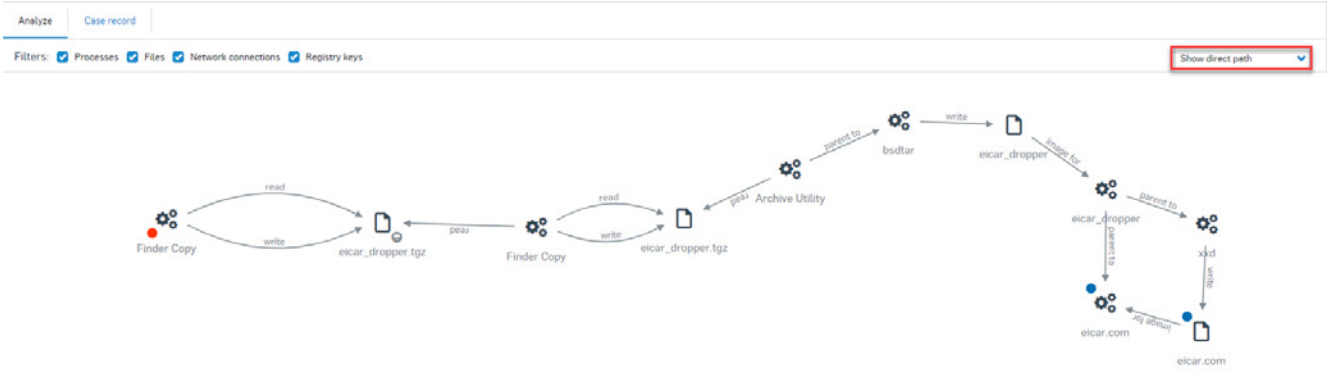

图 7: 威胁案例提供攻击链的可视交互表示。

整个网络安全环境的可见性

Sophos 提供 EDR 和 XDR（Extended Detection and Response，扩展侦测与响应），带来端点和服务器以及网络和电子邮件数据无与伦比的可见性。您可以从环境整体全盘视图概览快速切换到感兴趣的精细细节。这是行业顶尖防护水平，可阻止勒索软件等最新威胁，阻止漏洞利用攻击技术，阻挡黑客。

访问 www.sophos.cn/intercept-x 了解更多并开始免费试用

立即免费试用

30天免费试用
www.sophos.cn/interceptx

中国（大陆地区）销售咨询
电子邮件：salescn@sophos.com

2021-04-19 (MP)

SOPHOS