Sophos Network Detection and Response

监测网络流量，更快确定可疑活动

如果环境中出现攻击敌手，分秒必争。然而，有限的可见性和信息往往减缓防御者的速度。一旦安全工具不能很好地配合工作，情况将更加复杂。

最全面的数据推动最准确的侦测策略

全盘威胁侦测与响应方法，以及更快关联数量和种类越来越多的数据的方法，可以令企业获益。可见性和相关内容越深入，威胁活动调查越准确。这意味着安全遥测可以协助，更准确描绘整个攻击路线。

作为 Sophos MDR 的附加项，Sophos Network Detection and Response (NDR) 虚拟设备监测网络流量，来确定可疑网络流量。侦测结果发送到 Sophos 数据湖，评估，给定相应风险分数，并生成案例供 Sophos 威胁响应团队调查和验证。NDR 侦测可以触发对网络服务器内部连接的主机的调查，还可用于丰富端点活动的威胁追捕，确定通信的设备。

您的安全需要协同配合的工具

Sophos NDR 是原生 Sophos MDR 集成，因此其方便连接，不产生多余杂讯或不匹配的风险分数，也不像其他解决方案一样需要时间建立基线。下表介绍 Sophos NDR 侦测引擎的功能。

Sophos NDR 作为虚拟设备交付。部署后，通过 Sophos Central 管理控制台进行验证，然后开始发送数据。可以在 Sophos Central 中查看 NDR 状态和侦测结果。

亮点

- 将网络侦测加入 Sophos MDR，来监测端点软件无法访问的可疑网络流量
- 实现威胁调查并搜寻连线到网络服务和其他网络连接的内部主机
- 侦测通常隐藏的加密流量内的恶意软件
- 在 Sophos Central 中轻松查看 NDR 传感器状态和侦测结果

Sophos NDR 侦测引擎和使用案例

侦测引擎	说明
加密载荷分析 (EPA)	根据 session 大小、方向和到达间时间中发现的模式，侦测零日命令控制 (C2) 服务器以及新的恶意软件系列。
域生成算法 (DGA)	识别恶意软件用于回避侦测的动态域生成技术。
深度数据包检查 (DPI)	利用已知 IoC 监测加密和非加密流量，快速确定威胁黑客和 TTP。
Session 风险分析 (SRA)	强力逻辑引擎，利用规则对多种基于 session 的风险系数发出提醒。
设备侦测引擎 (DDE)	可扩展的查询引擎，利用深度学习预测模型，分析加密流量以了解不相关网络流量中的模式。

SOPHOS

识别端点以外的可疑行为

Sophos NDR 利用独立威胁侦测引擎，侦测以下可疑和异常网络流量行为：

- 来自未知设备的连接
- 远程 session 期间上传的数据
- 专有数据文件使用增多
- 恶意软件系列产生的网络session

借助侦测潜在恶意行为的能力，Sophos NDR 可识别：

- **未受保护的设备** – Sophos NDR 识别未受保护，可能被用作网络攻击入口点的合法设备。
- **恶意资产** – 除了监测未受保护的设备流量，Sophos NDR 还识别在网络中通信的未经授权设备。
- **IoT 和 OT 传感器** – 物联网 (IoT) 和运营技术 (OT) 设备给威胁监测带来挑战，因为许多此类设备无法支持端点保护代理。Sophos NDR 监测 IoT 和 OT 设备的数据以侦测攻击者活动。
- **零日攻击** – Sophos NDR 采用专利流程，根据 session 数据包大小、方向和间隔到达间时间中发现的模式侦测攻击者使用的零日 C2 服务器。
- **内部人员威胁** – Sophos NDR 提供最初在内部人员看来“正常”的网络流量和数据外泄可见性。

Sophos NDR 定价基于组织的用户和服务器总数。授权许可证包含虚拟设备软件。下表介绍 Sophos NDR 系统要求，快速学习攻击主体、内容、时间和方式。我们可以很快响应威胁。

Sophos NDR 系统要求

网络吞吐能力	1 Gbps	5 Gbps	10 Gbps
CPU	4	8	16
RAM	16 GB	32 GB	64 GB
存储	160 GB	320 GB	640 GB
预计用户范围*	最多 2,000	最多 10,000	最多 30,000

*将根据组织而变。

更多了解 Sophos NDR

sophos.com/ndr

中国（大陆地区）销售咨询
电子邮件：salescn@sophos.com

22-11-15 DS-ZHCN (DD)

SOPHOS