Sophos Network Detection and Response

Sophos XDR 和 Sophos MDR 的强大补充

Sophos NDR 与您的受托管端点和防火墙协同工作，监测它们未能发现的网络活动中的可疑和恶意模式。Sophos NDR 能够侦测来自非托管系统和 IoT 设备的异常流量、恶意资产、内部威胁、前所未见的零日攻击，以及网络深处的异常模式。

Sophos NDR 提供其他产品无法察觉的网络活动的关键可见性

攻击者擅长规避侦测，但每次攻击都需要在网络中移动。Sophos NDR 侦测您的受托管端点和防火墙未能发现的可疑网络流量模式，包括：

- **未知或未受保护的网络设备** – 包括无法用端点传感器完全管理的合法 IoT 或 OT 设备，以及网络上未知或未识别的系统。这些设备可能受到威胁或将受骇成为攻击的一部分。Sophos NDR 识别并监测此类设备中可能预示攻击的可疑或恶意行为。
- **未经授权或恶意资产** –Sophos NDR 很容易识别和监测引入网络的可能已经受骇或者用于启动攻击的资产加以。
- **新的和以前未见过的指挥与控制 (C2) 活动** – 许多攻击或入侵通过网络内恶意攻击者与远程进程之间看起来合法的沟通进行远程协调。Sophos NDR 能侦测新的零日 C2 活动，以识别可能刚刚开始的定制化目标攻击。
- **可疑或恶意的网络流量和模式**是早期识别网络攻击的重要信号。这些迹象可能包括非正常工作时间的网络活动或远程访问、可疑的数据上传或外泄、异常的流量模式以及已知恶意软件生成的恶意流量。

NDR 与您的防火墙协同工作

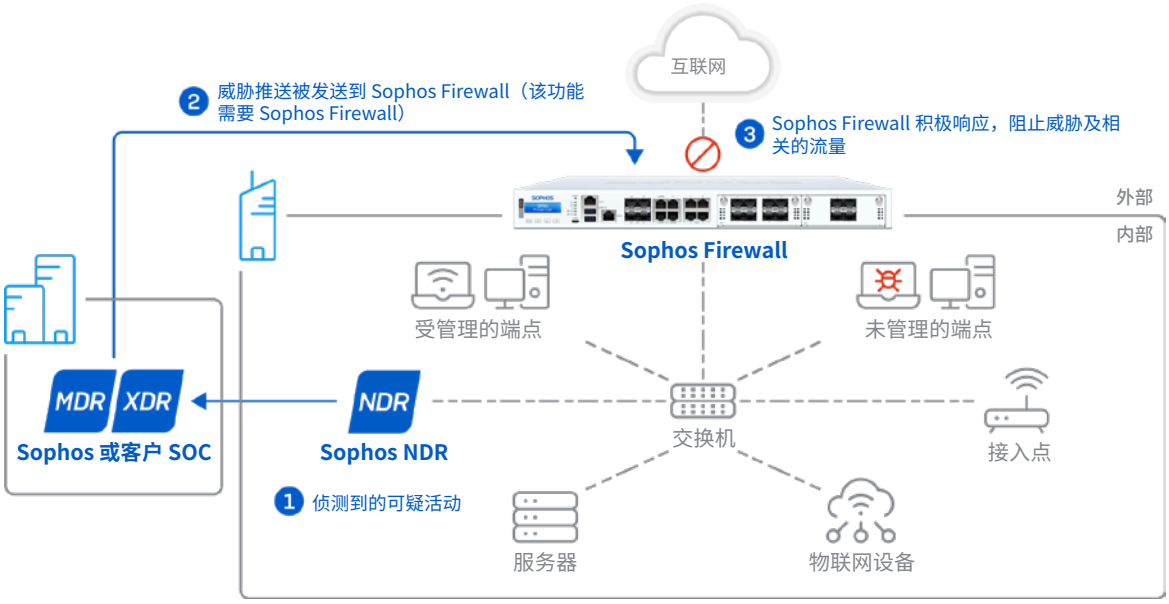
防火墙在保护网络边界和控制进出内容方面起到关键作用。Sophos NDR 是防火墙解决方案的完美补充，可以协同工作，提供防火墙看不到的网络深处的信息和覆盖。还包括可以特别地识别在内部网络中传递的可疑和恶意活动的技术，而这些活动在任何防火墙或端点防护产品都无法侦测到的。

亮点

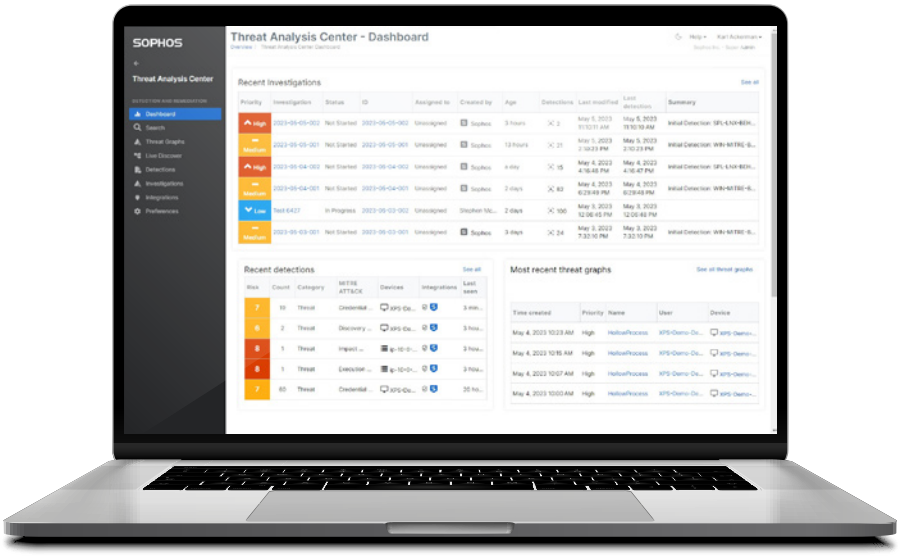
- 完美补充 Sophos XDR 和 MDR，提供对网络深层的侦测。
- 与您的防火墙协同，侦测网络活动和威胁。
- 侦测来自未知或未托管设备、不良资产和零日 C2 服务器的可疑网络活动。
- 检查加密流量，不会影响 PII。
- 从 Sophos Central 部署、配置和管理。
- 使用调查控制台深入了解可疑的网络活动，并分析或调查异常模式。

SOPHOS

Sophos NDR 在网络深处运行以侦测攻击



- 通过五个实时引擎深度监测网络内部的流量。
- 侦测所有网络资产的活动，包括未受托管的系统、IoT 设备和不良资产，识别这些设备的制造商、操作系统，以及其发出的任何可疑流量模式。
- 将数据和警报发送到 Sophos Central Data Lake 资料湖以及 Sophos 的 MDR SOC 团队或您的 XDR 团队。
- 通过易于使用的调查控制台，取得网络和应用活动、高风险流量以及可疑流量的可见性和深入信息。
- 如果您使用 Sophos Firewall，那么自动威胁响应可立即阻止威胁并防止横向移动。
- 作为虚拟设备运行在流行的 hypervisor 平台上，如 VMware 和 Hyper-V。
- 通过 SPAN 端口镜像直接连接交换机，监测所有流量。
- 检查加密数据包数据而不影响 PII 数据。



Sophos NDR 侦测引擎

Sophos NDR 包括 5 个侦测引擎，可以持续分析网络流量，运用 AI 机器学习分析，识别网络深处的可疑和恶意活动。

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 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)	强大的逻辑引擎利用规则来对以工作阶段为基础的风险因素发出警报。
设备侦测引擎 (DDE)	可扩展的查询引擎采用深度学习预测模型，分析不相关网络流量中模式的加密流量，并侦测端口扫描和 SSH 穷举破解行为。

Sophos NDR 授权许可

Sophos NDR 是 Sophos XDR 和 Sophos MDR 的完美补充，可作为一个集成套件使用。Sophos NDR 定价基于组织的用户和服务器总数。虚拟设备软件包含在授权许可证中，您可以根据需要部署任意多个 NDR 传感器。这比竞争对手按实例收费的方案更为经济和灵活。

Sophos NDR 技术规格

支持的平台

- VMware ESXi6.7 及更高版本
- Microsoft Hyper-V 6.0.600118016 (Windows Server 2016) 或更高版本
- Amazon AWS c5n.2xlarge
- 经认证的硬件

硬件	最大吞吐量	最大连接数/秒	处理器	内存
Dell R660 (双插槽)	40Gbps	120K	64	128GB
Dell R660 (单插槽)	40Gbps	80K	32	64GB
Dell R650	20Gbps	40K	24	64GB
Dell R450	10Gbps	20K	16	32GB
Dell R350	4Gbps	8K	8	32GB
Intel Nuc 第 13 代	2.5Gbps	4K	12	32GB

VM 系统要求

Sophos NDR VM 支持每个传感器高达 1Gbps：

- 对中等流量使用默认 VM 设置：
  - 高达 500Mbps
  - 高达 70,000 个数据包 / 秒
  - 高达 1,200 个流秒
- 对于高流量，调整 VM 实现 8 个 vCPU：
  - 高达 1Gbps
  - 高达 300,000 个数据包 / 秒
  - 高达 4,500 个流秒

其他资源：

- Sophos NDR 社区资源
- 通过 Sophos 网络侦测与响应 (Sophos Network Detection and Response, NDR) 增强安全运营
- 经认证的硬件规格

要了解更多信息，请访问：

www.sophos.com/ndr

中国（大陆地区）销售咨询
电子邮件：salescn@sophos.com

24-12-19 DS-ZHCN (MP)

SOPHOS