解决方案概要

# Sophos MDR

## 24/7 专家主导的威胁防御


Sophos 托管式侦测与响应 (MDR) 是由专家提供的全托管服务，它们专责侦测并响应针对您的计算机、服务器、网络、云工作负载、电子邮件账户、备份等的网络攻击。我们的高级安全分析师能够阻止高级人工主导的攻击，并在威胁影响您的业务运营或危害敏感数据之前，采取即时行动加以消除。

## 使用案例

### 1 | 全天候威胁监控

**期望结果：**通过拥有能够代表您应对威胁的专家，扩展您的 IT 和安全团队。

**解决方案：**Sophos MDR 安全分析师全天候监控、调查并响应威胁，执行即时的人工主导响应行动，阻止已确认的威胁。Sophos 拥有 500 多名威胁侦测与响应专家，并由七个全球安全运营中心提供支持。

### 2 | 加速威胁响应

**期望结果：**改善对已确认威胁的平均响应时间 (MTTR)。

**解决方案：**Sophos MDR 分析师可以代表您执行威胁响应行动，以阻断、遏制并消除攻击者，行业领先的平均威胁响应时间为 38 分钟，比行业基准快 96%。

### 3 | 拦截安全工具未能识别的威胁

**期望结果：**侦测出比安全工具自身能识别的更多的网络威胁。

**解决方案：**65% 的勒索软件攻击始于攻击者利用合法用户凭证或未知漏洞，而 29% 则始于泄露的凭证。Sophos MDR 分析师执行主动威胁搜索，以识别只有人类才能侦测到的攻击者行为，并迅速消除仅靠工具无法阻止的威胁。

### 4 | 提高投资回报

**期望结果：**整合您整个环境中的安全解决方案，并从技术投资中获得更高的 ROI。

**解决方案：**Sophos MDR 可以提供所需技术，或充分利用您现有的网络安全投资来侦测和响应威胁。Sophos 的开放式 AI 原生平台可以收集、过滤并关联来自众多网络安全和 IT 工具的数据，使 Sophos MDR 分析师能够以快速、准确和透明的方式消除已确认的威胁。

## 同行认可

Gartner Peer Insights Customers' Choice 2024

*Sophos 在 2024 年 Gartner® 托管式侦测与响应客户之声报告中获评为“客户之选”*

G2 Leader

*由 G2 上的客户评价和评论的最高评分托管式侦测与响应服务*

## 行业认可

MITRE ATT&CK

*在 MITRE ATT&CK Evaluations for Managed Services 中表现优异的厂商*

**了解更多，获取定制的服务建议 Sophos MDR:**
www.sophos.com/MDR



2025-02-03 SB-ZHCN (PC)

SOPHOS