Sophos Rapid Response

立刻应对攻击中的威胁

Sophos Rapid Response 由事件应对专家团队快速协助识别和消除针对您企业的作用中的威胁

遭遇攻击时分秒必争

应对攻击中的威胁时，从最初攻破迹象到完全消除威胁之间的时间越短越好。随着敌人逐步展开攻击，您需要与时间赛跑，确保他们无法得逞。

通过 Sophos Rapid Response，我们帮助您快速脱离危险，24/7 全天候远程事件应对、威胁分析和威胁追踪专家团队可以：

- 快速采取措施识别、隔离和消除作用中的威胁
- 将敌人挡在企业之外，避免进一步破坏您的资产
- 执行持续 24/7 全天候监测和应对，增强您的防护
- 建议实时预防措施，解决根本原因
- 在企业内快速部署 Sophos 云技术产品
- 分析第三方技术的补充数据
- 提供事件结束后的详细威胁总结，说明我们的调查结果

Sophos Rapid Response 的产品特点

Sophos Rapid Response 具有 Sophos MDR Complete 的所有优势以及一些其他优势。

	Sophos Rapid Response
MDR Complete“授权”威胁应对模式	✓
24/7 全天候侦测、追踪和应对	✓
在作用中的威胁期间的专门应对负责人和直接电话接入	✓
分析第三方技术的补充数据	✓
快速报价和当天帐户激活	✓
事件结束后正式总结详细说明调查	✓

产品亮点

- 快速识别和消除作用中的威胁
- 事件应对和 24/7 全天候监测（为期 45 天）
- 专门联络点和应对负责人
- 事件结束后的威胁总结，详细说明采取的所有措施
- 可预测定价，包含固定成本，无隐藏费用
- 以可保险理赔而设计
- 在Sophos Rapid Response之后，无缝整合到Sophos Managed Detection and Response（MDR）订阅。

SOPHOS

消除作用中的威胁

Sophos Rapid Response 团队是消除作用中威胁的专家。无论是感染、攻破还是尝试绕过安全控制的未经授权访问资产，我们都能够发现并阻止。

我们的事件应对专家团队隶属于 Sophos Managed Detection and Response (MDR) 方案，24/7 全天候威胁追踪、侦测和应对服务作为全托管服务的一部分，代表客户主动追踪、识别、调查并应对威胁。

定额收费

传统事件应对 (IR) 服务按小时计费，存在低估完全消除威胁所需时间的风险，这样您可能需要购买额外时间，更糟糕的是，刺激传统 IR 服务可能有增加应对所需时间的倾向。

Sophos Rapid Response 采用固定费用定价模式，无隐藏成本，由企业的用户和服务器数量决定。远程提供服务，这样我们可以在第一天就启动应对措施。由于时间不再是成本，尽快帮助您摆脱危险符合我们和您的利益。

快速部署

为了确保尽可能最快应对，Sophos 快速部署流程关注 Sophos MDR 代理直接分布到可发现的端点和服务器。

制定利用移除工具替代现有产品的替换策略后，部署工程师远程团队咨询每个 Rapid Response 客户发起定制行动计划，将自动化工具用于网络上的大规模部署。

团队协作，优化网络中的 Sophos MDR 代理运行状况，确保最佳做法配置以加快调查。

Rapid Response 方法

Rapid Response 获批并且客户接受我们的服务协议后，我们将直接采取行动。Rapid Response 包括四个主要阶段 – 接洽、分类、消除和监测。

接洽 (Onboarding)

- 主持人会启用电话会议，拟订沟通方式，确认已经采取的补救措施（如果有）
- 确定攻击规模和影响
- 共同制定应对计划
- 开始部署服务软件

分类 (Triage)

- 评估运行环境
- 确定已知的威胁或对手活动迹象
- 执行数据收集和启动调查工作
- 协同发起应对工作的计划

消除 (Neutralize)

- 移除攻击者的访问权
- 阻止资产或数据的进一步损失
- 阻止数据进一步外泄
- 建议实时预防措施，解决根本原因

监测 (Monitor)

- 过渡到 MDR Complete 服务
- 执行持续监督，侦测复发情况
- 提供事件后的威胁汇总答复

详细威胁汇总

消除针对您企业的作用中的威胁后，我们将为您提供正式调查总结，详细说明我们所采取的措施，发现，以及未来避免发生类似威胁的长期指导建议。

事件后的 24/7 全天候监测和响应

解决事件并消除对企业的直接威胁后，我们可转换您来到顶级 MDR 服务 MDR Complete，提供随时主动威胁追踪、调查、侦测和应对。

如果威胁再次发生或出现新威胁，我们可随时应对，无需您额外付费。如果您遭受攻击 45 天，我们将在订购期内为您防御 45 天。

正遇到外泄？

请随时拨打下面的地区电话，联系事件顾问 (Incident Advisors)。

澳大利亚 +61 272084454

奥地利 +43 73265575520

加拿大 +1 7785897255

法国 +33 186539880

德国 +49 61171186766

意大利 +39 02 94752 897

英国 +44 1235635329

美国 +1 4087461064

瑞典 +46 858400610

瑞士 +41 445152286

如果所有事件顾问均繁忙没空，请留言，将有专人尽快回复您。

正遇到外泄？

有关更多信息，请访问
www.sophos.cn/rapidresponse

中国（大陆地区）销售咨询
电子邮件：salescn@sophos.com

23-02-01 DS-ZHCN (PC)

SOPHOS