SOPHOS

Rapid Response 常见问题及解答

必须现有 Sophos 客户才能成为 Rapid Response 服务客户吗?

不。现有 Sophos 客户和非 Sophos 客户均可以享受 Sophos Rapid Response 服务。

我遇到主动攻击，应该怎么办?

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

美国 +1 4087461064

澳大利亚 +61 272084454

加拿大 +1 7785897255

法国 +33 186539880

德国 +49 61171186766

英国 +44 1235635329

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。

Rapid Response 服务有多快?

非常快。事实上大多数客户会在数小时内得到接洽，48 小时内得到分类。由于服务完全远程进行，可以在联系 Sophos 后数小时内开始响应。

接洽(onboarding) 流程是什么?

Rapid Response 团队可以在收到批准后开始接洽流程并启动调查。对于环境中没有安装 Sophos Intercept X 的企业，Sophos 提供了快速部署 (Rapid Deployment) 选项。快速部署团队擅长在当前经历活动事件的环境中进行快速安装。

快速部署收取额外费用吗?

不，快速部署是整个服务的一部分。

快速部署方法是什么?

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 MTR Advanced 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

提供哪些语言版本的 Rapid Response?

目前该服务的服务语言仅为英语。

Sophos 能够与 Data Forensic Incident Response 服务 (DFIR) 一起工作或替代它吗?

Sophos 可以与 DFIR 服务一起工作，已经在多个场合实现。Sophos Rapid Response 专注于 DFIR 服务的事件响应方面，并不提供传统 DFIR 项目通常提供的所有服务。

Sophos 会实际提供设备吗？所有事件响应者会前往客户所在地?

不，所有事件响应均远程进行。

客户必须在端点安装 Sophos 吗?

是的。Rapid Response 采用标准 Managed Threat Response / Intercept X Advanced with EDR 代理程序提供，确保我们可以提供有效的 24/7 全天候监测与响应。这意味着他们无需卸载或临时禁用当前的非 Sophos 端点防护。

Rapid Response 团队不需要等待部署完成，就可以开始采取补救措施，隔离和消除威胁。团队将利用任何现有数据，借助适合辅助响应的工具。

如何报价?

报价基于用户和服务器总数，以 45 天固定期限报价。

有任何额外费用吗?

没有，服务无任何隐藏费用。

Rapid Response 期限结束后怎样?

期限结束后，客户可以切换为完全 Sophos Managed Threat Response (MTR) 客户，或者许可证将到期。

可以在一部分环境部署 Rapid Response 吗，或者整个环境必须在部署范围内?

在部分情况下，Rapid Response 可以仅应用于一部分客户环境。Rapid Response 专家可以提供更多详细信息作为项目范围的一部分。

Sophos 可以与代表客户的合同中间人合作吗，如法律公司?

是的。可以与中间人合作。

Sophos 可以确定攻击中外泄/失窃的文件吗?

Rapid Response 服务尽最大努力确定（如果有）攻击中已外泄的文件，但并不保证这一点，因为这取决于调查中提供的数据。

Sophos 将代表客户解密勒索软件吗?

不，这不是 Rapid Response 服务的内容。

Sophos 帮助客户协商或协调赎金支付吗?

不，这不是 Rapid Response 服务的内容。

中国（大陆地区）销售咨询
电子邮件: salescn@sophos.com

2021-03-08 FAQ (PS)

SOPHOS