Sophos Rapid Response

よくある質問 (FAQ)

Rapid Response サービスを利用するには、ソフォスの既存の顧客である必要はありますか?
いいえ。Sophos Rapid Response サービスは、ソフォスの既存のお客様とソフォス以外 (ソフォス製品をお持ちでない) のお客様の両方が利用できます。

アクティブな侵害が発生しています。次に何を行えばいいですか?
以下の地域の番号へ連絡をすることで、いつでもインシデントアドバイザーと話すことができます。

米国 +1 4087461064

オーストラリア +61 272084454

カナダ +1 7785897255

フランス +33 186539880

ドイツ +49 61171186766

英国 +44 1235635329

スウェーデン +46 858400610

イタリア +39 0287317993

Rapid Response サービスの速さはどれくらいですか?
非常に速いです。お客様の大部分は数時間でオンボーディングされ、48 時間で優先順位付けされます。サービスは完全にリモートなので、ソフォスに連絡してから数時間以内に対応することが出来ます。

オンボーディングプロセスとは何ですか?
Rapid Response チームは、承認を得るとすぐに、オンボーディングプロセスを開始し、調査を始めることができます。お客様の環境に Sophos XDR がインストールされていない組織向けに、ソフォスは Rapid Deployment のオプションを提供しています。Rapid Deployment チームは、現在アクティブなインシデントが発生している環境に迅速インシデント対応活動を展開できる専門家です。

Rapid Deployment に関して追加料金はかかりますか?
いいえ。Rapid Deployment はサービスの一部として含まれています。

Rapid Response のサービスとは何ですか?
Rapid Response が承認され、お客様がサービス利用規約に同意した後、すぐにお使いいただけます。Rapid Response には、オンボーディング、トリアージ (優先付け) 、無効化、監視の主に 4つのカテゴリーがあります。

オンボーディング

- ホストのキックオフコールで通信設定を確立し、どのような修復手順 (もしある場合) がすでに実行されているかを確認
- 攻撃の規模と影響を特定
- 対応計画を相互に定義
- サービスソフトウェアの導入を開始

トリアージ

- 運用環境を評価
- 既知の感染の痕跡や悪意のあるアクティビティを特定
- データ収集を実行し、調査活動を開始
- 応答アクティビティを開始するための計画を共に作成

無効化

- 攻撃者のアクセスを排除
- アセットやデータへのさらなる損傷を停止
- さらなるデータの流出を防止
- 問題に取り組むためのリアルタイムの予防措置を推奨

SOPHOS

Sophos Rapid Response のよくある質問

監視

- MDR Advanced サービスへの移行
- 継続的な監視を実行して、再発を検出
- インシデント後の脅威の概要を提供

Rapid Response はどの言語で提供されていますか？
現在、このサービスは英語のみとなります。

ソフォスは、デジタルフォレンジック・インシデントレスポンス (DFIR) との連携または置き換えはできますか？
ソフォスは、DFIR サービスと連携して、複数の契約を行ってきています。Sophos Rapid Response は、DFIR サービスのインシデントレスポンスの側面に焦点を当てており、従来の DFIR 契約で通常提供されるすべてのサービスを提供するわけではありません。

ソフォスは物理的に装置を出荷していますか？ インシデント対応担当者はお客様の場所に行きますか？
いいえ。すべてのインシデント対応はリモートで行われます。

お客様は、エンドポイントにソフォス製品をインストールする必要がありますか？
はい。Rapid Response は、Managed Detection & Response / Sophos XDR を使用して、効率的に 24 時間 365 日体制の監視と対応を提供できるようにします。つまり、現在のソフォス以外のエンドポイント保護をアンインストールするか、一時的に無効にする必要があります。

Rapid Response チームは、脅威を封じ込み、無効化するための是正措置を開始する前に、インストールが完了するのを待つ必要はないのです。チームは、利用可能なデータを活用し、インシデント対応に適したツールを使用します。

価格はどのように設定されますか？
価格は、ユーザー数とサーバー数の合計に基づいており、45日間の固定期間として価格が設定されています。

追加コストはかかりますか？
いいえ。サービスに追加コストはかかりません。

Rapid Response のサービス期間が終了した後はどうなりますか？
期間の終了時に、お客様は正式な Sophos MDR (Managed Detection & Response) サービスのライセンスに移行してください。それをしない場合は、ライセンスの有効期限が切れます。

Rapid Responseを環境の一部に展開することは可能ですか、それとも環境全体がスコープに含まれなければならないのでしょうか？
Rapid Responseは、お客様の環境の一部分にしか適用できない場合もあります。Rapid Response の専門家は、プロジェクト範囲の一部として詳細を提供できます。

ソフォスは、契約上法律事務所などの顧客を代表する仲介業者と連携することはできますか？
はい。仲介業者との連携は可能です。

ソフォスは、攻撃で流出した / 盗難されたファイルを特定できますか？
Rapid Response サービスでは、攻撃の一部として流出したファイルを特定するためのベストエフォート（最善の努力）が含まれています。ただし、調査の一環として入手可能なデータによる可能性があるため、このことを保証は出来ません。

ソフォスはお客様の代わりにランサムウェアを復号化しますか？
いいえ。これは Rapid Response サービスの一部ではありません。

ソフォスは、お客様に代わり身代金支払いの交渉または円滑に進める支援しますか？
いいえ。これは Rapid Response サービスの一部ではありません。

2022-09-14 (FAQ-PC)

SOPHOS