SOPHOS

Rapid Response - Questions fréquentes

Dois-je être client de Sophos pour bénéficier du service Rapid Response ?

Non. Le service Sophos Rapid Response est ouvert à la fois aux clients actuels et aux non-clients de Sophos.

Je subis actuellement une violation active, que dois-je faire ?

Appelez le numéro ci-dessous correspondant à votre pays pour être mis en relation avec l'un de nos conseillers.

USA +1 408 746 1064

Australie +61 272 084 454

Canada +1 778 589 7255

France +33 1 86 53 98 80

Allemagne +49 611 711 86 766

Royaume-Uni +44 1235 635 329

Si tous les conseillers en incidents (Incident Advisors) sont occupés, veuillez laisser un message et quelqu'un vous rappellera dans les plus brefs délais.

Quelle est la rapidité du service Rapid Response ?

Extrêmement rapide. La majorité des clients sont pris en charge en quelques heures et font l'objet d'une priorisation sous 48 heures. Le service étant fourni à distance, la réponse peut commencer quelques heures seulement après le premier contact avec Sophos.

En quoi consiste le processus de prise en charge des clients ?

L'équipe Rapid Response peut entamer le processus de prise en charge et commencer son investigation dès qu'elle en reçoit l'autorisation. Pour les entreprises qui n'ont pas Sophos Intercept X installé dans leur environnement, Sophos offre une option de déploiement rapide. L'équipe du déploiement rapide (Rapid Deployment) est experte en installations rapides dans les environnements qui connaissent un incident actif.

Faut-il prévoir un coût supplémentaire pour le déploiement rapide ?

Non. Le déploiement rapide est inclus dans le service.

Quelle est la méthodologie du service Rapid Response ?

Une fois que le service Rapid Response a été approuvé et que le client a accepté le contrat de service, nous intervenons immédiatement. La réponse comporte 4 étapes principales : prise en charge, priorisation, neutralisation et surveillance.

Prise en charge (Onboarding)

- Premier contact pour établir les préférences de communication et confirmer les mesures correctives (le cas échéant) qui ont déjà été prises
- Identification de l'ampleur et de l'impact de l'attaque
- Définition mutuelle d'un plan d'intervention
- Déploiement du logiciel du service

Priorisation (Triage)

- Évaluation de l'environnement opérationnel
- Identification des indicateurs de compromission connus et des activités malveillantes
- Collecte de données et lancement de l'investigation
- Élaboration d'un plan de lancement des activités de réponse en concertation avec le client

Neutralisation (Neutralize)

- Suppression de l'accès des attaquants
- Neutralisation de toute autre atteinte aux actifs ou aux données
- Prévention de toute nouvelle exfiltration de données
- Recommandation d'actions préventives en temps réel pour remédier aux causes profondes

Surveillance (Monitor)

- Transition vers le service MTR Advanced
- Suivi continu pour détecter toute récidive
- Livraison d'un compte-rendu post-incident de la menace

Dans quelles langues le service Rapid Response est-il disponible ?

Le service est actuellement uniquement disponible en anglais.

Sophos travaille-t-il avec ou remplace-t-il les services Data Forensic Incident Response (DFIR) ?

Sophos peut travailler conjointement aux services DFIR et l'a fait dans le cadre de multiples opérations. Sophos Rapid Response se concentre sur la partie 'réponse aux incidents' des services DFIR et ne fournit pas tous les services généralement offerts dans le cadre d'une investigation DFIR traditionnelle.

Sophos va-t-il envoyer du matériel par la poste ? Les opérateurs Sophos se déplacent-ils sur le site du client ?

Non. La réponse aux incidents est toujours effectuée à distance.

Les clients doivent-ils installer Sophos sur leurs postes de travail ?

Oui. Rapid Response est fourni en exploitant le service Managed Threat Response Standard et l'agent Intercept X Advanced with EDR pour garantir une surveillance et une réponse efficaces 24 h/24 et 7 j/7. Cela signifie qu'ils devront également désinstaller ou désactiver temporairement leur protection Endpoint non-Sophos.

L'équipe Rapid Response n'a pas besoin d'attendre la fin du déploiement pour commencer à prendre des mesures correctives afin de contenir et de neutraliser la menace. L'équipe exploitera toutes les données disponibles et utilisera les outils appropriés pour faciliter la réponse.

Comment le prix du service est-il calculé ?

Le prix est basé sur le nombre total d'utilisateurs et de serveurs et est fixé pour une durée de 45 jours.

Faut-il prévoir des coûts supplémentaires ?

Non. Le service n'a pas de coûts cachés.

Que se passe-t-il après la période de 45 jours du service Rapid Response ?

À la fin de la période de 45 jours, les clients peuvent choisir d'évoluer de façon permanente vers le service Sophos Managed Threat Response (MTR), ou de laisser la licence expirer naturellement.

Pouvons-nous déployer Rapid Response seulement sur un segment de l'environnement, ou faut-il que l'intégralité de l'environnement soit intégrée dans le service ?

Dans certaines situations, Rapid Response peut ne s'appliquer qu'à un segment de l'environnement du client. Un spécialiste Rapid Response vous fournira plus d'informations lors de la planification du service.

Sophos peut-il travailler sur le contrat avec un intermédiaire représentant le client, tel qu'un cabinet d'avocats ?

Oui. Il est possible de travailler avec un intermédiaire.

Sophos peut-il déterminer quels fichiers ont été exfiltrés/volés lors de l'attaque ?

Le service Rapid Response fait tout son possible pour déterminer quels fichiers (le cas échéant) ont été exfiltrés dans le cadre d'une attaque. Toutefois, cela n'est pas garanti car cela dépend des données analysées dans le cadre de l'investigation.

Sophos déchiffrera-t-il au nom du client les fichiers affectés par un ransomware ?

Non. Cela ne fait pas partie du service Rapid Response.

Sophos aidera-t-il le client à négocier ou à faciliter le paiement d'une rançon ?

Non. Cela ne fait pas partie du service Rapid Response.

Équipe commerciale France
Tél. : 01 34 34 80 00
Email : info@sophos.fr

2021-03-08 FAQ (PS)

SOPHOS