Sophos Rapid Response

Häufig gestellte Fragen

Muss ich bereits Sophos-Kunde sein, um den Rapid Response Service in Anspruch nehmen zu können?
Nein. Sophos Rapid Response steht sowohl Sophos-Kunden als auch Nichtkunden zur Verfügung.

Ich bin von einem aktiven Sicherheitsvorfall betroffen. Was mache ich jetzt?
Kontaktieren Sie uns bitte auf Englisch über eine der beiden folgenden Optionen:

- per E-Mail an **RapidResponse@sophos.com**

- telefonisch über folgende Rufnummer:
  +49 611 711 867 66 (D/AT/CH)

Die Rufnummern für alle anderen Regionen finden Sie unten.

Die KollegInnen sind 24x7 erreichbar. Falls gerade alle Experten im Gespräch sind, erreichen Sie nach 2 Min. die Voicebox. Bitte hinterlassen Sie Ihren Namen, Ihre Rufnummer und eine kurze Beschreibung des Vorfalls in englischer Sprache. Sie erhalten dann so schnell wie möglich einen Rückruf.

Rufnummern für andere Regionen:

USA/weltweit: +1 4087461064

Frankreich: +33 186539880

UK: +44 1235635329

Australien: +61 2720844454

Kanada: +1 7785897255

Wie schnell reagiert der Rapid Response Service?
Sehr schnell. Das Onboarding der meisten Kunden erfolgt binnen weniger Stunden und die Triage ist in der Regel nach 48 Stunden abgeschlossen. Da der Service vollständig remote ist, können bereits wenige Stunden nach Kontaktaufnahme mit Sophos Reaktionsmaßnahmen ergriffen werden.

Wie läuft der Onboarding-Prozess ab?
Das Rapid-Response-Team kann mit dem Onboarding-Prozess und ersten Analysen beginnen, sobald Sie Ihre Genehmigung erteilt haben. Für Unternehmen, die Sophos XDR nicht in ihrer Umgebung installiert haben, bietet Sophos mit Rapid Deployment eine schnelle Bereitstellung an. Das Rapid-Deployment-Team ist auf schnelle Installationen in Umgebungen spezialisiert, die gerade von einem aktiven Vorfall betroffen sind.

Fallen zusätzliche Gebühren für die schnelle Bereitstellung an?
Nein. Rapid Deployment ist Teil des Service.

Wie ist die Vorgehensweise bei Rapid Response?
Nachdem Rapid Response genehmigt wurde und der Kunde unseren Service-Vertrag akzeptiert hat, werden wir sofort aktiv. Es gibt bei Rapid Response vier Hauptphasen – Onboarding, Triage, Neutralisierung und Monitoring.

Onboarding

- Erstgespräch zum Klären der Kontaktpräferenzen und ggf. bereits getroffener Reaktionsmaßnahmen
- Bestimmen von Ausmaß und Auswirkungen des Angriffs
- Gemeinsames Festlegen eines Reaktionsplans
- Bereitstellung der Service-Software

Triage

- Bestandsaufnahme der Betriebsumgebung
- Aufspüren bekannter Kompromittierungs-Indikatoren oder Angriffsaktivitäten
- Datenerfassung und Einleitung von Analyse-Aktivitäten
- Gemeinsame Erarbeitung eines Plans zum Ergreifen von Reaktionsmaßnahmen

SOPHOS

Sophos Rapid Response – häufig gestellte Fragen

Neutralisierung

- Blockieren des Angreifer-Zugriffs
- Verhinderung weiterer Schäden an Assets oder Daten
- Unterbindung weiterer Daten-Exfiltrationen
- Empfehlung von Präventiv-Maßnahmen in Echtzeit

Monitoring

- Umstellung auf den MDR Advanced Service
- Kontinuierliches Monitoring, um ein erneutes Auftreten zu erkennen
- Bedrohungs-Bericht nach dem Vorfall

In welchen Sprachen wird Rapid Response angeboten?
Derzeit wird der Service nur auf Englisch angeboten.

Kann Sophos mit oder anstelle von Data Forensic Incident Response Services (DFIR) eingesetzt werden?
Sophos kann parallel zu DFIR-Services eingesetzt werden und wird auch bereits oft so genutzt. Sophos Rapid Response konzentriert sich auf den Incident-Response-Aspekt von DFIR-Services und bietet daher nicht alle Leistungen eines traditionellen DFIR-Service.

Versendet Sophos Equipment? Reisen Response-Experten zum Kundenstandort?
Nein. Die gesamte Reaktion auf Vorfälle erfolgt per Remote-Zugriff.

Müssen Kunden Sophos auf ihren Endpoints installieren?
Ja. Rapid Response nutzt den Managed Detection & Response/Sophos XDR Agent, damit wir 24/7 effektive Monitoring- und Reaktionsmaßnahmen ergreifen können. Deshalb müssen Kunden außerdem Sophos-fremde Endpoint-Security-Software deinstallieren oder vorübergehend deaktivieren.

Das Rapid-Response-Team kann schon vor Abschluss der Bereitstellung Maßnahmen zum Eindämmen und Beseitigen der Bedrohung ergreifen. Das Team nutzt alle verfügbaren Daten und greift auf Tools zur Unterstützung der Reaktionsmaßnahmen zurück.

Wie wird der Preis berechnet?
Der Preis richtet sich nach der Gesamtzahl der Benutzer und Server und gilt als Festpreis für 45 Tage.

Fallen zusätzliche Kosten an?
Nein. Bei dem Service gibt es keine versteckten Kosten.

Was geschieht nach Ablauf der Rapid-Response-Phase?
Am Ende der Laufzeit können Kunden entweder zu Sophos Managed Detection & Response (MDR) wechseln oder die Lizenz läuft ab.

Kann Rapid Response in nur einem Segment der Umgebung implementiert werden oder muss die Implementierung in der gesamten Umgebung erfolgen?
In bestimmten Situationen kann Rapid Response nur auf ein Segment der Kundenumgebung angewendet werden. Ein Rapid-Response-Spezialist kann Ihnen im Rahmen der Projektplanung weitere Details nennen.

Kann Sophos mit einem Vermittler (z. B. Anwaltskanzlei) zusammenarbeiten, der den Vertrag im Auftrag des Kunden abschließt?
Ja. Die Arbeit mit einem Vermittler ist möglich.

Kann Sophos feststellen, welche Dateien beim Angriff exfiltriert/gestohlen wurden?
Im Rahmen des Rapid Response Service unternehmen wir alle Anstrengungen, um festzustellen, ob, und wenn ja, welche Dateien im Rahmen eines Angriffs exfiltriert wurden. Wir können jedoch keine lückenlosen Informationen über Exfiltrationen garantieren, da diese Erkenntnisse von den im Rahmen der Analyse verfügbaren Daten abhängig sind.

Entschlüsselt Sophos Ransomware für den Kunden?
Nein. Diese Leistung ist im Rapid Response Service nicht enthalten.

Hilft Sophos dem Kunden, Lösegeld-Zahlungen auszuhandeln oder abzuwickeln?
Nein. Diese Leistung ist im Rapid Response Service nicht enthalten.

2022-09-14 (FAQ-PC)

SOPHOS