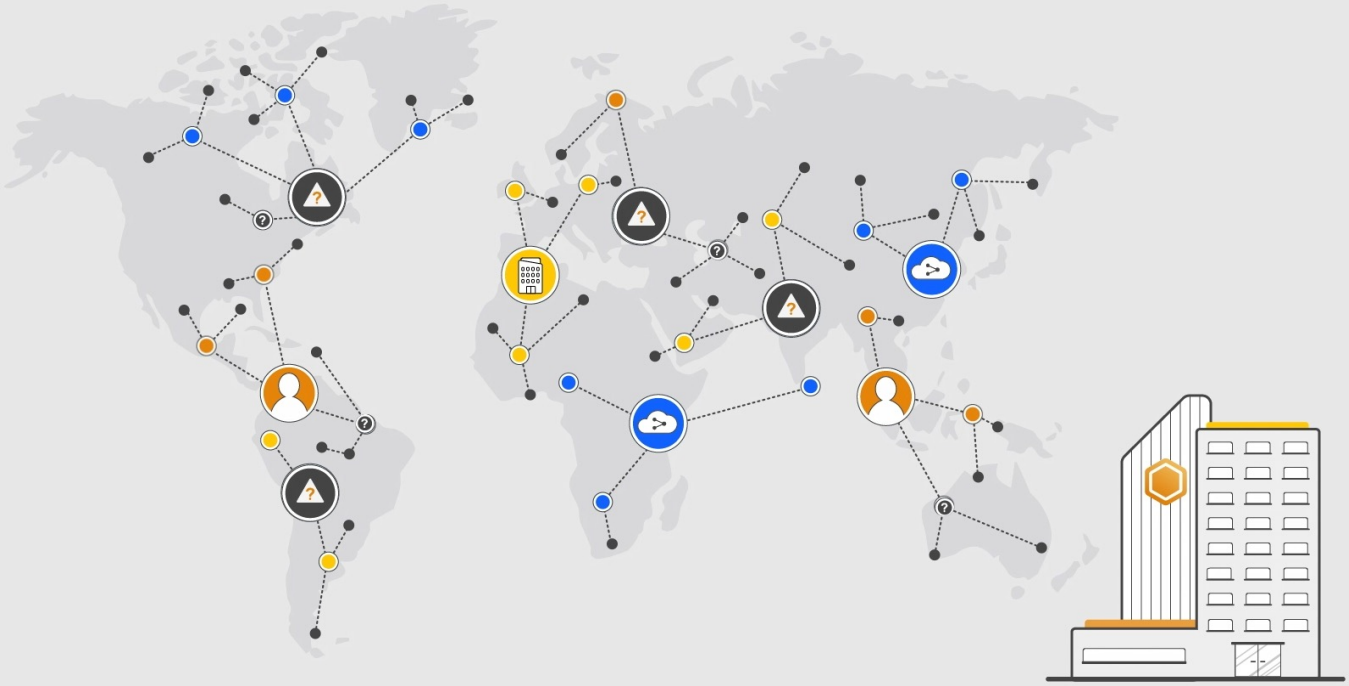
HoneyTrace

Trace. Detect. Respond.



USE CASE

Third Party and Supply Chain Assessment

Your data travels worldwide. Does your security?

There has been a rapid increase in the volume of confidential and sensitive data third parties and the supply chain are responsible for.

Once you provide these parties with this critical data, and it has left your internal network, you often have no visibility on how your data is stored and who has access to it. The more suppliers you have, the more vulnerable your data is. How do you know your data remains safe?

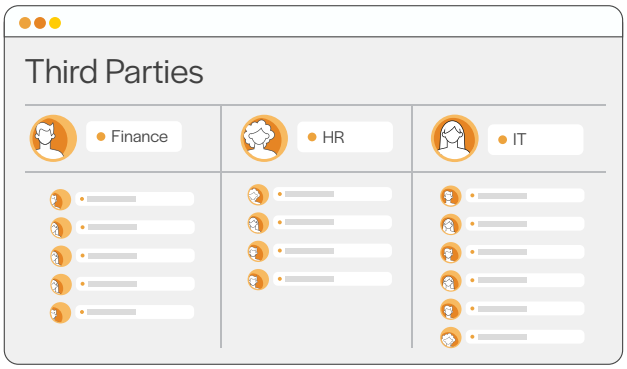
HoneyTrace can help you discover risks with third party providers and your supply chain, by tracking your data as it leaves your network boundary.

Discovering Third Party and Supply Chain Risks

Sarah has been tasked by her executive to complete an assessment and identify any data risks their third party providers, consultants, contractors, outsourced support and other elements of the supply chain pose to the organisation. These partners hold considerable volumes of confidential and sensitive data, which if lost, will have significant impact on the organisation. Once this data has left Sarah's internal network, she has no visibility on how her important data is stored and who has access to it.

Sarah decides to employ HoneyTrace, to help her complete a data risk assessment.

For this assessment, Sarah's team selects a sample of real documents typically shared with third parties and within the supply chain. Each document is uploaded to HoneyTrace, and tracking methods are inserted, so the team can monitor the movement of the documents beyond their network boundary.



STEP 1

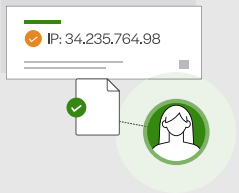
Create a list of candidates

Sarah's team begins by contacting internal departments, who exchange sensitive data with partners, to create a list of third parties that are suitable for assessment.

Individuals from each internal department (Finance, HR & IT) are nominated as a point of contact (POC). These representatives are asked to identify an upcoming data exchange that can be included in the assessment.

Each contact is asked to record the expected behaviour of the data exchange, such as, where it should be stored and who should have access.

Identifying expected behaviour



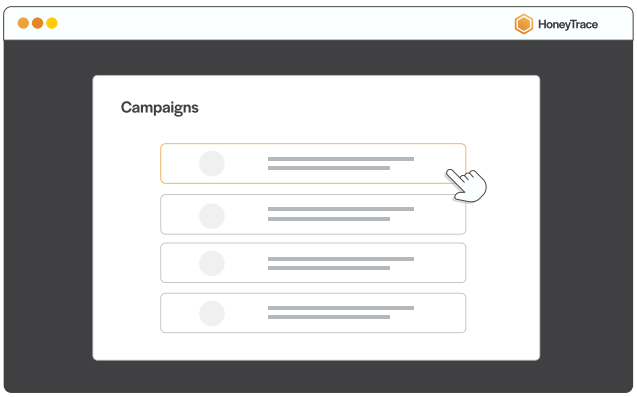
As these documents are intended to be accessed, it will be normal for alerts to be triggered. To manage these alerts, it is important to separate the alerts into expected vs unexpected behaviour. Through conversations and contractual arrangements, develop a preferred view on where the files should be accessed and stored. This will help you keep track of locations where the files should be legitimately accessed i.e the third party's office network.

To triage your alerts, you will need to determine the IP and user agent string that will be considered 'expected behaviour'. These could be identified from the first alert you receive. Rules can then be created to mute these alerts.

STEP 2

Create a Third Party campaign

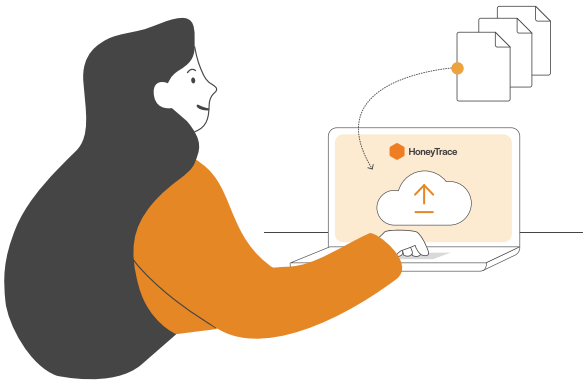
Sarah's team accesses HoneyTrace and creates a Third Party campaign, so they can track the document activity in a central place.



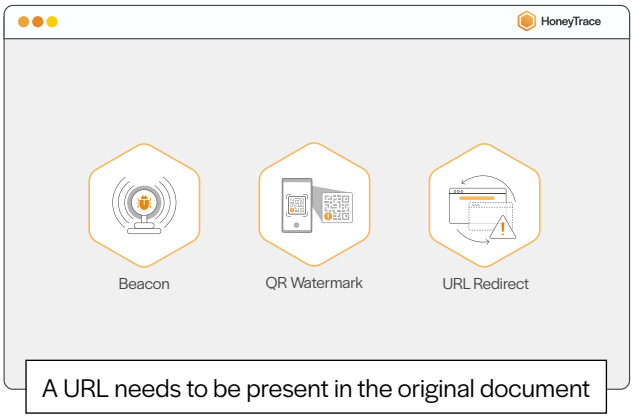
STEP 3

Upload files and configure tracers

Sarah's team upload the documents which need to be tracked. Office documents such as docx, pptx and xlsx can be uploaded into HoneyTrace.



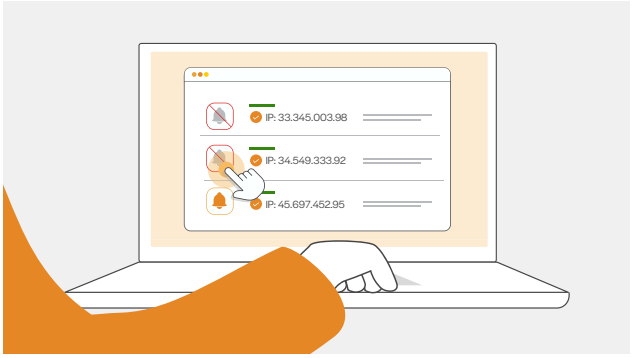
Tracers are added to each document, to track their movement around the third party and supply chain networks. For this scenario, we recommend selecting the URL redirect, QR Code Watermark and Thinkst Canary tracers. To configure a URL redirect, your original document will need to contain a web address.



STEP 4

Distribute and remove documents

The documents are downloaded from HoneyTrace and distributed to each of the third parties through the organisation's normal methods of transferring data. After the documents are distributed, the team then deletes the original files from HoneyTrace. Despite the deletion, the document metadata is retained for ongoing file tracking.



STEP 5

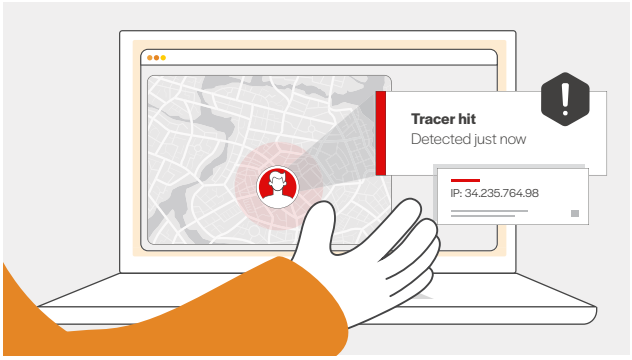
Create alert rules

To avoid alert fatigue, Sarah's team enables rules to mute any alerts that are triggered by expected behaviour. They begin by muting any alerts that are triggered by the third party's office network IP.

STEP 6

Identify suspicious behaviour

Unexpected or suspicious behaviour may indicate that an individual has accessed the document external to their office network, has distributed the file to others outside of their organisation or the third party's network has been compromised.



Within a week, Sarah's team traces the movement of a document from a third party to a suspicious association and identifies a data breach. Sarah reports the risks to the executive and works with the third party to strengthen their data protections.