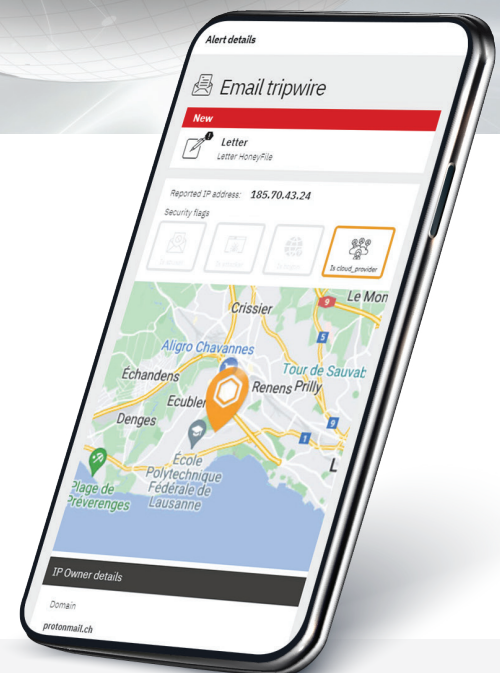


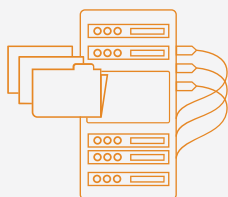
## Data loss detection beyond your network boundary

**HoneyTrace allows you to track your sensitive data inside and outside your network perimeter, so you can understand where your data goes and if it's at risk of a data leak.**

HoneyTrace works in the cloud and in places beyond your control. It's ideal for verifying how your partners and employees are managing your data.

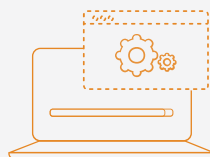


## HoneyTrace combines multiple tracking techniques into one solution



### Simple to use

Integrates seamlessly into your existing cybersecurity systems



### No installation

No need to install or manage additional software packages



### Enterprise scalable

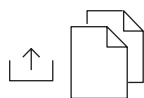
Detect and trace data leaks throughout every department and beyond



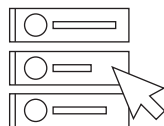
Reduce data loss risks with this simple to use, cost-effective, enterprise scalable, no install solution, which can be deployed in minutes.



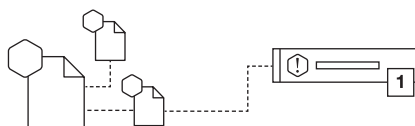
## How HoneyTrace works



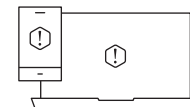
Upload document or create digital twin



Select one or more tracers



Upload Honeytrace files into environment



Receive an alert

## Understanding insider attacks or human error:

Privileged users and administrators (insiders) have approved access to the operating systems and have knowledge of corporate security measures. Due to these reasons, they can view or transfer sensitive information without an alert. These breaches and data theft may go undetected for months, if not years.

You can use HoneyTrace to generate artificial files and place them in a location that is only accessible by essential users. If they are accessed, a tracer will be triggered, and you will receive a notification. This may indicate that an employee may be abusing their position within the organisation by looking at content outside their required day-to-day activities or their credentials have been compromised.

## Identifying third party providers and supply chain risks:

For many organisations, globalisation has meant a rapid increase in the volume of data that Third Party providers and the Supply Chain is responsible for. While many cybersecurity products provide protection for internally managed data, it remains, however, a longstanding business challenge of how to effectively understand how these partners manage the data that they are entrusted to store, process, and manage.

Once you provide these third parties with this critical data and it has left your internal network, you often have no direct access to the information or visibility on how the data is stored and who has access to it.

HoneyTrace will enable you to track and know when your data has been accessed outside of your network.



Scan the QR code to learn more