USE CASE: DETECTING MALICIOUS EMPLOYEES

A lawyer at a top firm in Manhattan was about to be terminated. One morning, DatAlert triggered a warning about unusual access to idle and sensitive data—the attorney in question was hijacking the firm's most sensitive case files.

The maligned attorney had approved access, but Varonis knew it was abnormal for him to be accessing hundreds of files and folders that he hadn't touched in years.

How does Varonis detect when a malicious employee starts stealing data they have access to?

Varonis knows which data people have access to, whether that data is sensitive, and what their normal file and email access activity looks like, making it possible to detect rogue admins and disgruntled employees.

If a user accesses data that they personally haven't used in a while (i.e., "idle data"), it could be an indication of account compromise, a malware infection, or that the user is starting to accumulate data prior to their departure or some other event.

Likewise, an employee that touches an increasing amount of sensitive data compared to their typical behavior could indicate that they're looking for valuable data to steal or delete, or that their account has been hijacked.

Relevant DatAlert threat models

- Abnormal behavior: accumulative increase in access to idle data
- Abnormal behavior: accumulative increase in access to idle and sensitive data