ASCEMA

Data Discovery Executive Summary

Created On:	08/08/2019
From:	01/01/2019
To:	31/07/2019
Duration:	212 days
Interval:	Monthly

Table of Contents

Risk Profile

Reporting Period: 01/01/2019 – 31/07/2019
Comparable Period: 04/06/2018 – 31/12/2018

Found

213
instances of sensitive data

£25,347
estimated value of the discovered data*

+77%

Resolved

203
instances of sensitive data were resolved

£24,157
estimated value of the mitigated risk*

+55%

Outstanding

101
instances of sensitive data are outstanding

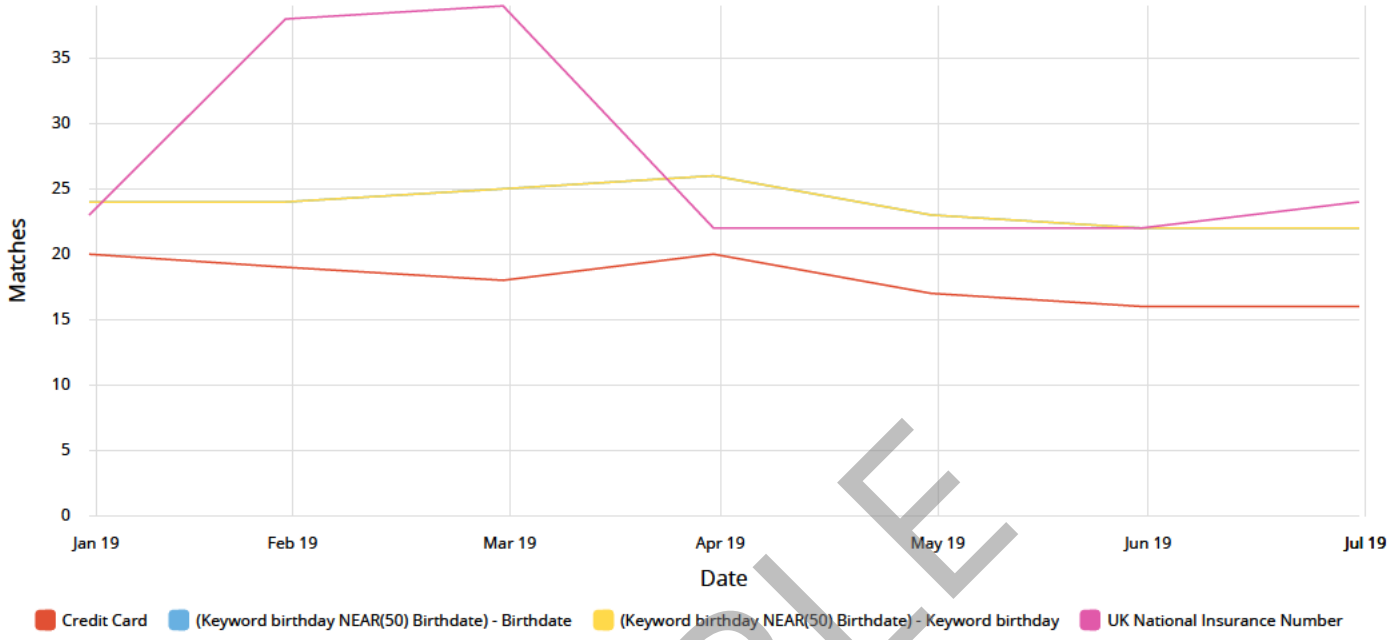
£12,019
estimated value of the risk exposure*

+23%

* Figures taken from the 2018 Cost of a Data Breach Study by Ponemon https://www.ibm.com/security/data-breach

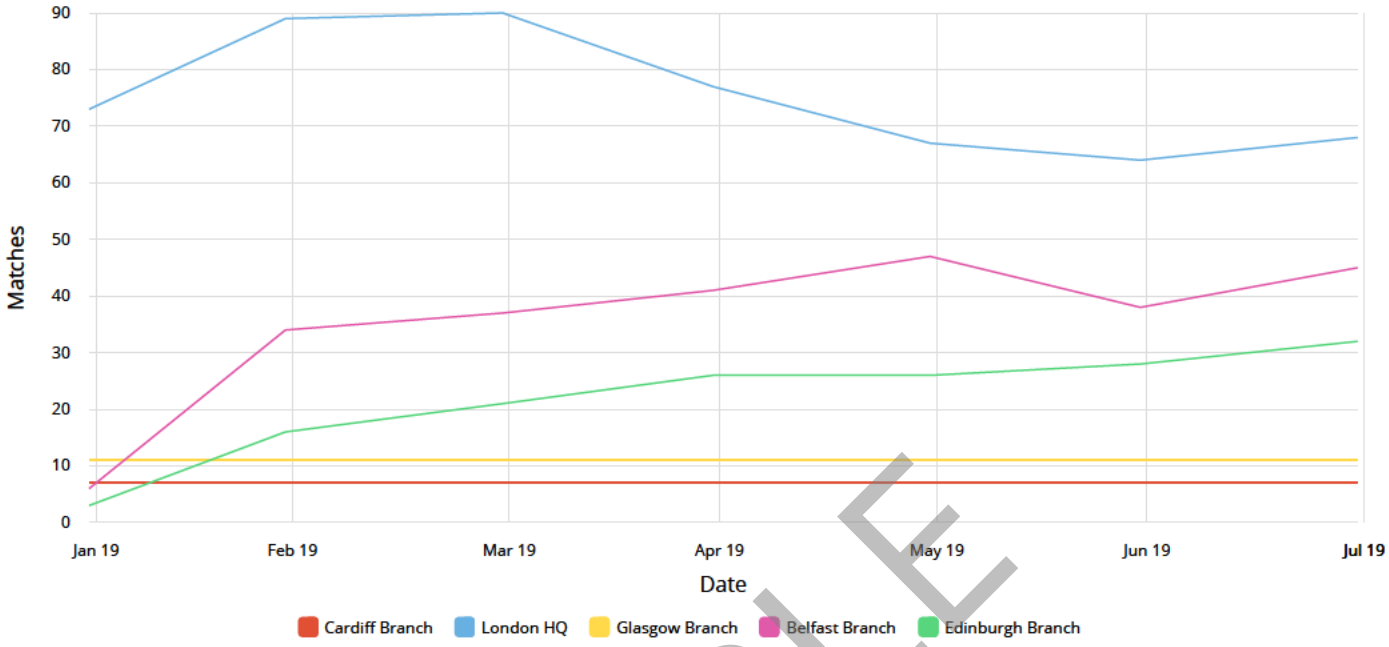
Top 4 Patterns

This graph displays the top 4 patterns found by search task and how that has changed over time. Search tasks can be configured with different priorities, confidence levels, matches and filters, so may not be directly comparable depending on how they have been set up on the system.



Total Matches by Location

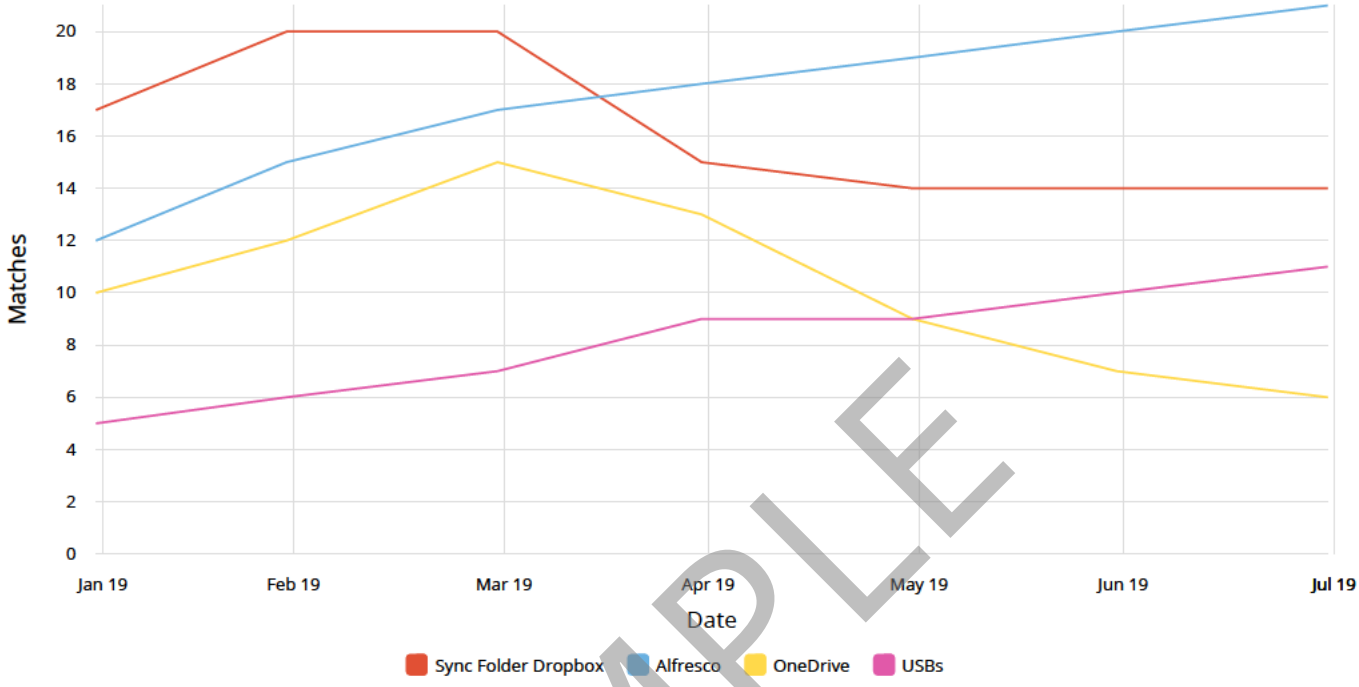
This graph displays the number of matches that were found in each location and how that has changed over time. Depending on organisational structure, these locations may not be directly comparable in size or activity.



Where sensitive data has been found › Key Risk Areas

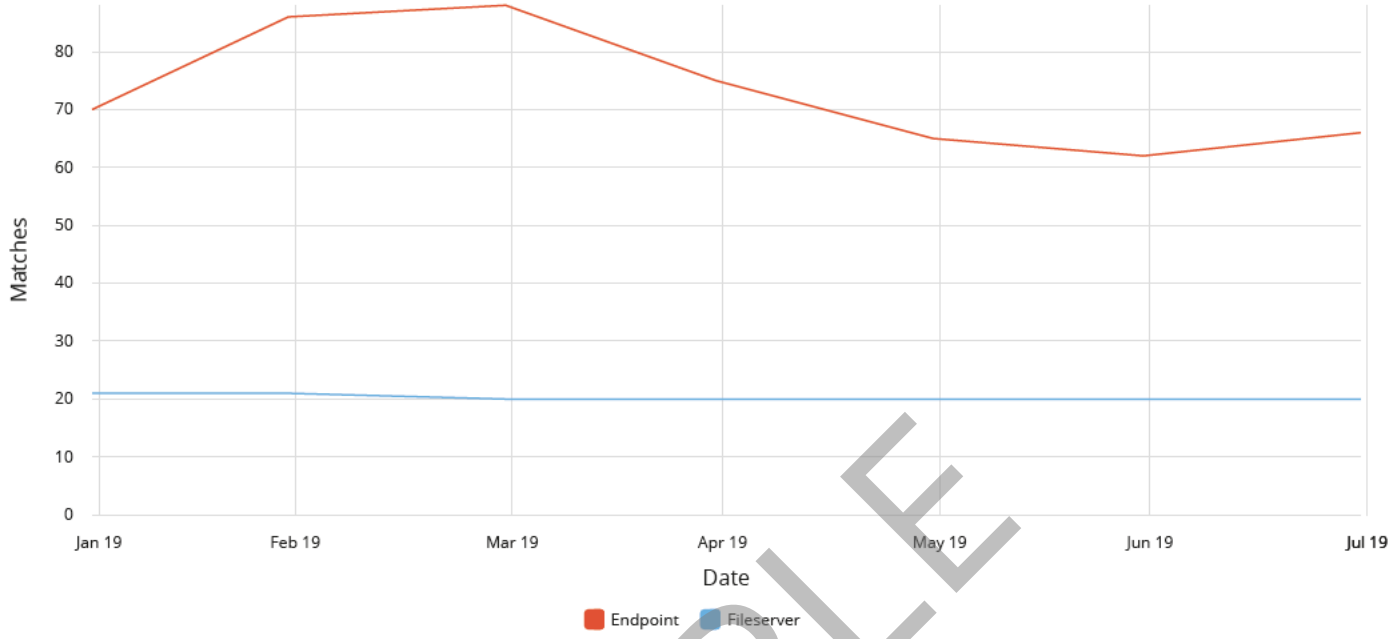
Total Matches by Key Risk Area

This graph displays the number of matches found in areas considered key risk and how that has changed over time. Depending on company policies, there may be a preference as to where sensitive data should or should not be stored. The graph displays where this data has been found and how this has changed over time. Data may have been found via scheduled search routines or as a result of real time monitoring.



Total Matches by Device Type

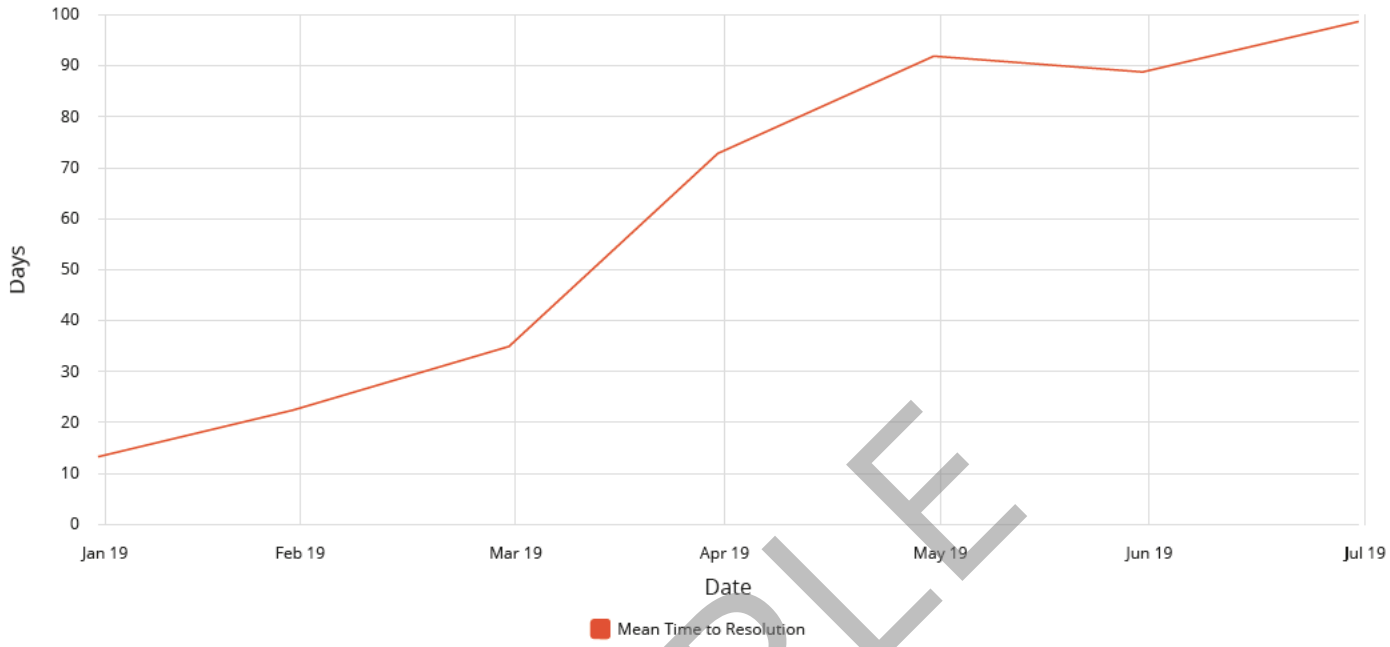
An Endpoint is typically the computer used by the end user e.g PCs and laptops. A File Server is typically a server that can be accessed by more than one user. Depending on company policies, there may be a preference as to where sensitive data should or should not be stored. This graph shows where this data has been found and how that has changed over time.



Mean Time to Resolution

This graph measures the average elapsed time in days from when a match is found and alerted, to when it is confirmed resolved.

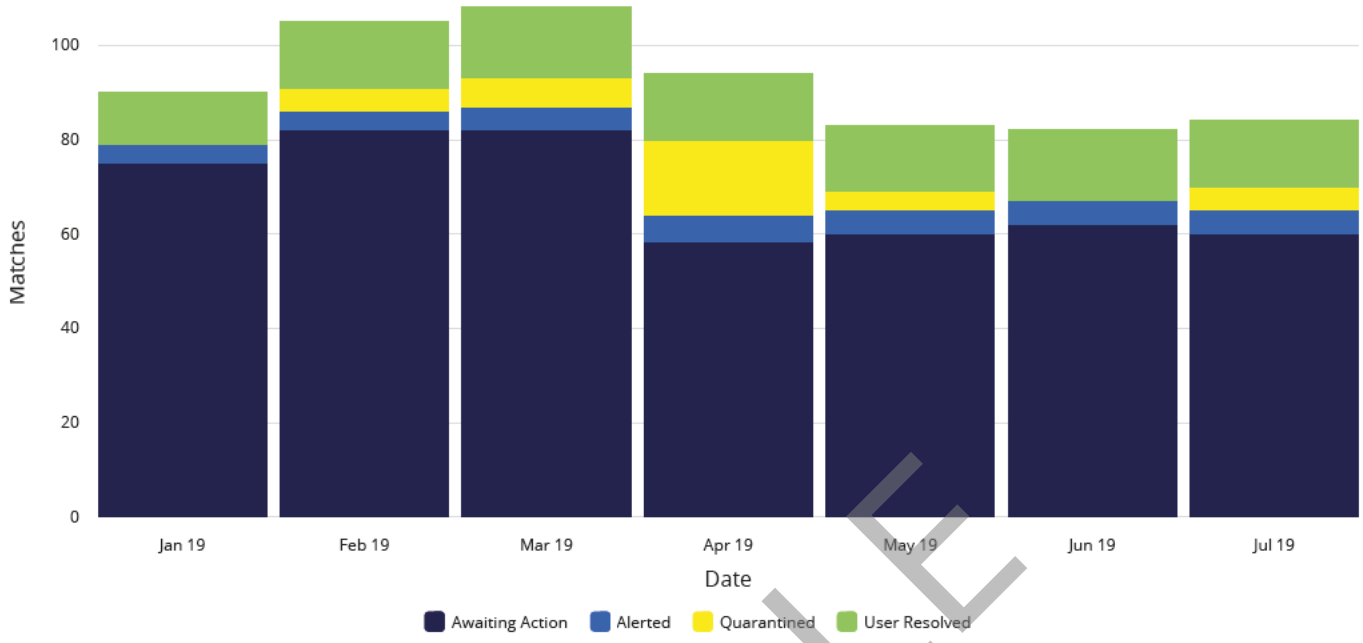
As an example, GDPR requires that simple Subject Access Requests are responded to within one calendar month*. If the MTTR is higher than this then it could indicate a problem.



* https //ico org uk/your-data-matters/time-limits-for-responding-to-data-protection-rights-requests/

Outstanding Matches

This graph shows a cumulative total of all matches that have not yet been confirmed resolved. The matches are split by their current status within the system.



Awaiting Action
– Matches found across all tracked files that have not been alerted to the end user yet.

Alerted
– Matches that have been alerted to the end user.

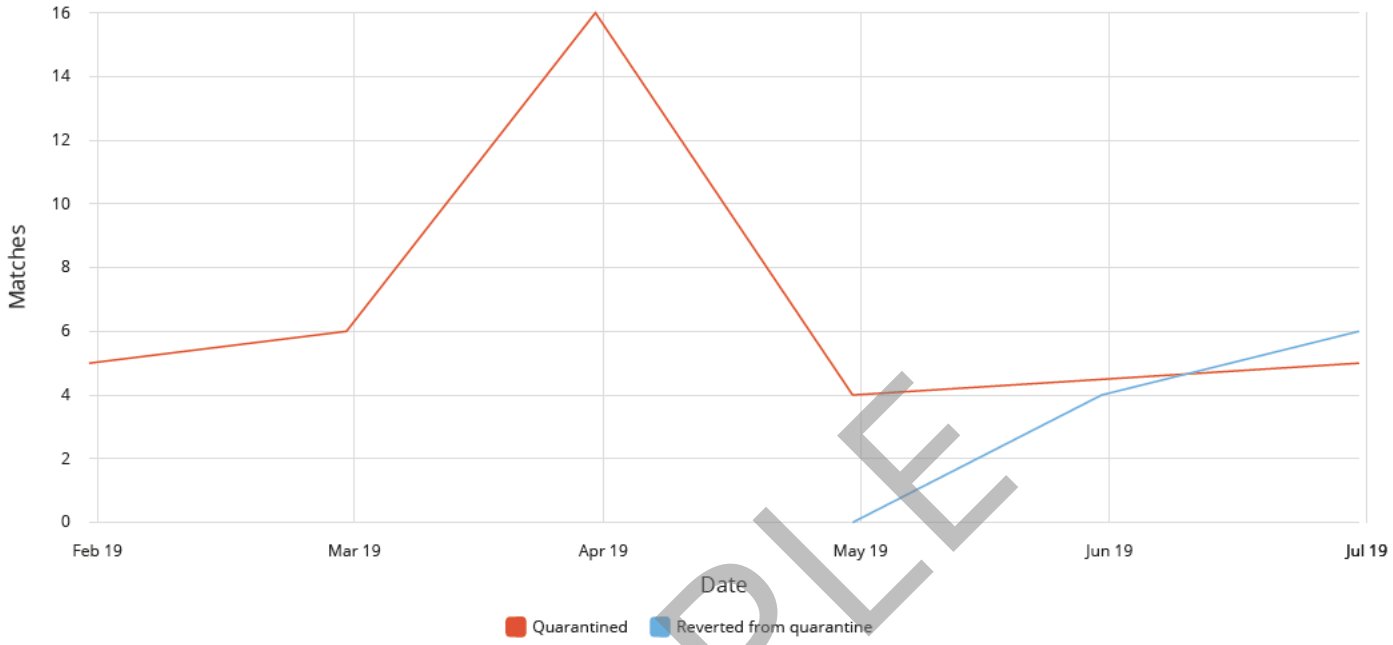
User Resolved
– Matches that have been removed, ignored or otherwise dealt with by the end user.

Quarantined
– Matches that have been placed into quarantine.

Quarantined Matches

In order to help you manage sensitive data from being released there is a facility to quarantine files which contain such data. This means that the file will no longer be available on the device. After a file has been placed in quarantine, it can be resolved by either releasing it from quarantine and allowing it to be held on the device or it can be deleted.

A file may contain more than one match, but quarantining an item can only be carried out at file level.



Pattern
– a predefined or user defined set of characters, words or an example document e.g a Credit Card number, person's name or an HR form.

Search Task
– a scheduled or real time routine set up by the administrator to monitor files across the enterprise to check if they contain sensitive Patterns.

Match
– content within a file that meets the criteria set in the Search Task as defined by the administrator. A file may contain multiple Matches.

Alert
– an automated or manual notification sent to the end user by the system or administrator to inform them that they have potentially sensitive data on their device as a result of a Match.

Contact

More information on GeoLang's Ascema Data Discovery tool, as well as a 30-day free trial, can be found at www.geolang.com.