Understanding breach alerts with Aman

Aman - Dark Web Monitoring · https://www.aeserver.com/support/understanding-breach-alerts-with-aman/

Your Dark Web Breach Report shows what Aman has found, how serious it is, and what to do next. This guide explains each part of the report so you can read it with confidence.

Opening your report

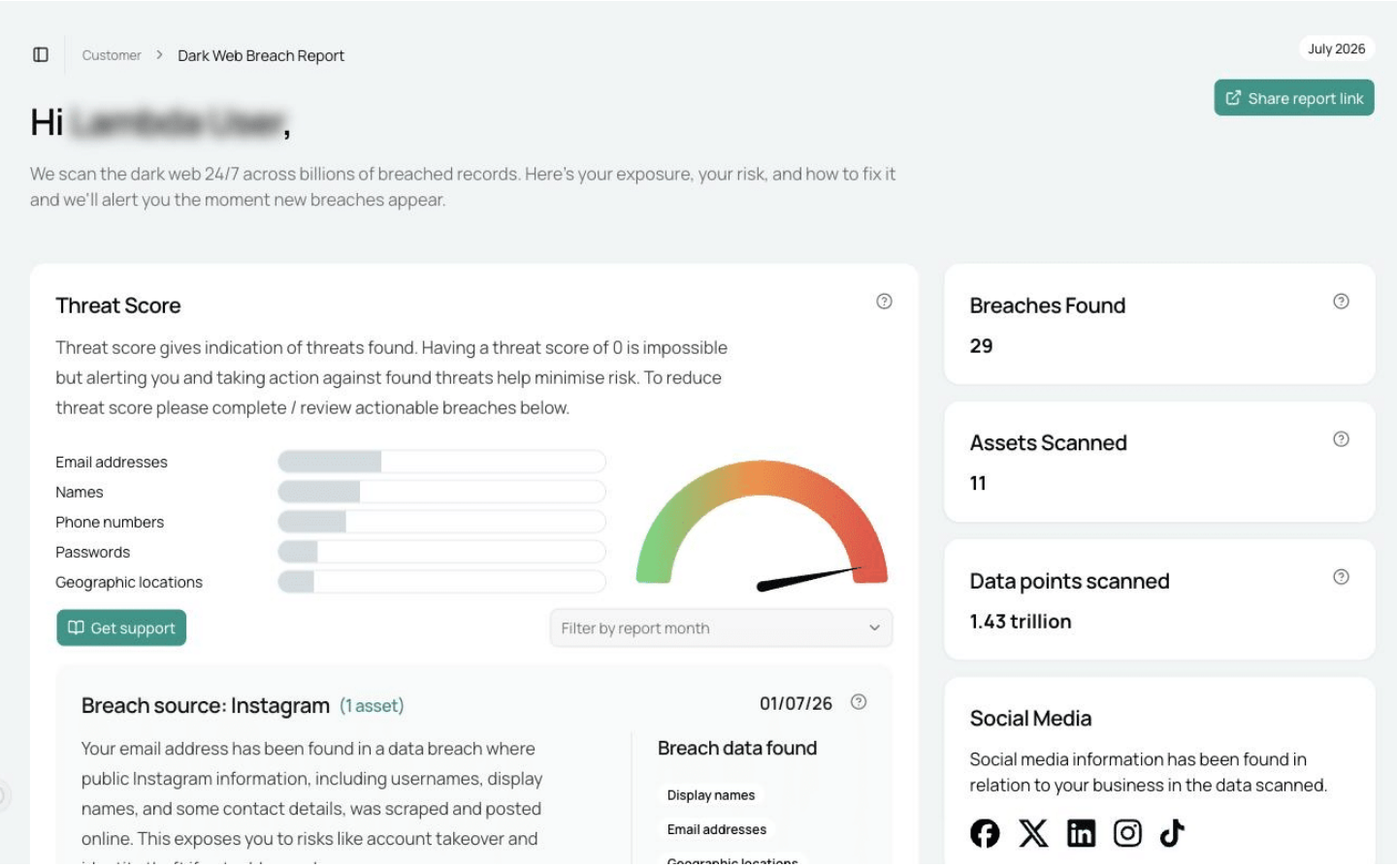
From your Aman dashboard in the AEserver client area, select **Login to Aman** or **Dark Web Breach Report**. In the portal, the left sidebar has two items: **Dark Web Breach Report** and **Knowledge Base**.

The report covers one month at a time. The current month is shown at the top right, and **Filter by report month** lets you look at earlier periods.

The summary figures

At the top of the report you will find:

Figure	What it tells you
Breaches found	How many separate breaches include one or more of your monitored assets.
Assets scanned	How many of your domains and email addresses were checked.
Data points scanned	The volume of leaked records searched on your behalf.
Social media	Whether social media information relating to your business appeared in the data scanned.
Credit cards	Whether any payment card information relating to your business was found.



The top of your Dark Web Breach Report: threat score, breaches found, assets and data points scanned.

Threat score

The threat score is an indication of your overall exposure, shown as a gauge. Underneath it, your exposure is broken down by category:

- Email addresses
- Names
- Phone numbers
- Passwords
- Geographic locations

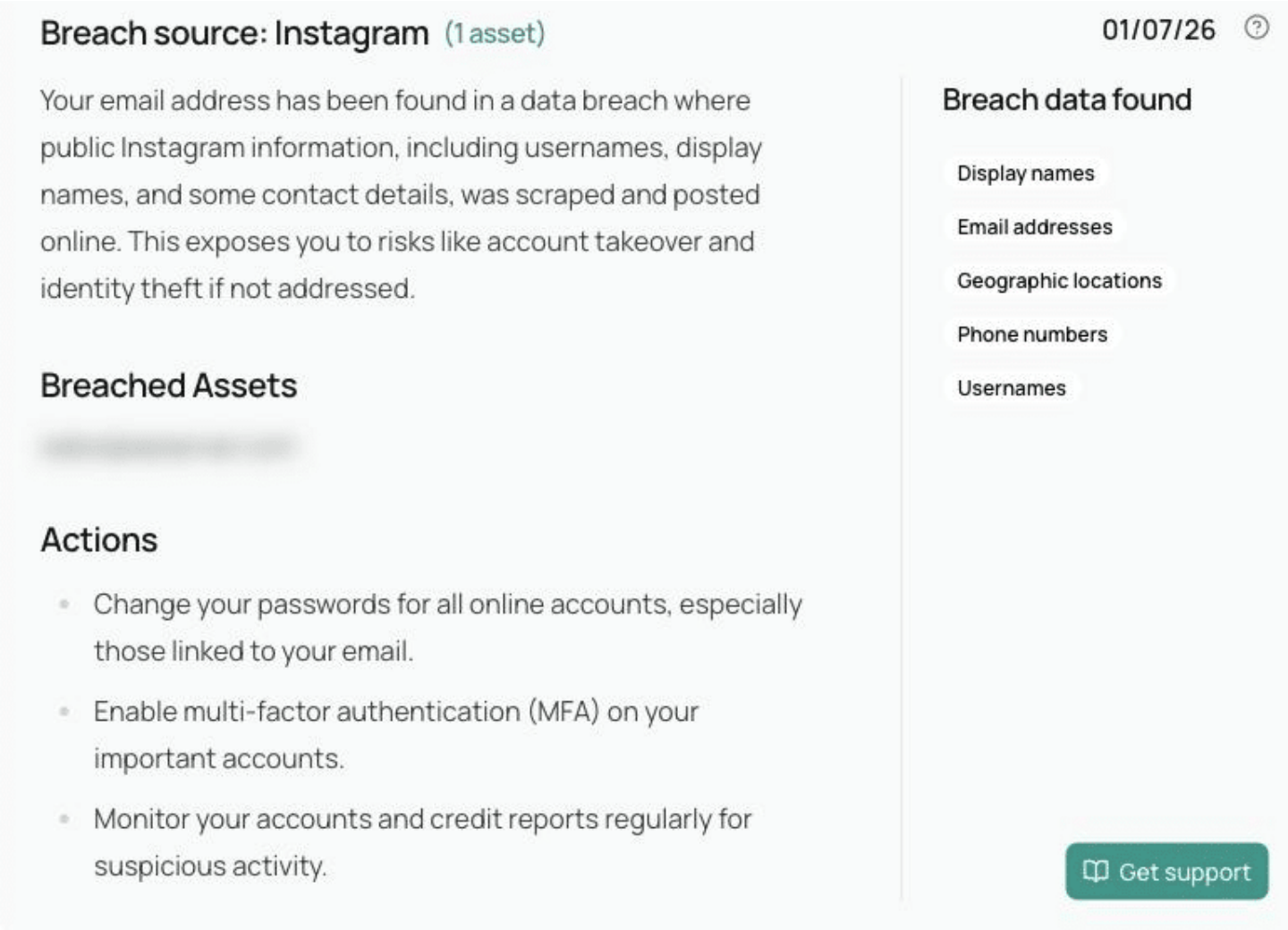
A score of zero is not achievable, because past breaches cannot be undone. The score is there to show you where your exposure is concentrated and to fall as you work through the actions on each finding.

There is no button to mark a finding as resolved Your score responds to you completing the recommended actions in the real world, such as changing an exposed password. Reviewing the findings and acting on them is what reduces your risk.

How to read a single finding

Each breach appears as its own card. A card contains:

Part of the card	What it means
Breach source	The name of the service or dataset the leaked data came from.
Asset count	How many of your monitored assets appeared in this particular breach.
Date	When the breach data is dated. Older dates are common and expected.
Description	A plain English explanation of what was exposed and why it matters.
Breached Assets	Exactly which of your email addresses were found in this breach.
Actions	The specific steps to take for this finding.
Breach data found	The categories of information exposed in this breach.
Get support	Opens support if you are unsure what the finding means.



A single breach finding: source, date, description, affected asset, actions and the data that was exposed.

Types of data Aman reports

The categories shown under **Breach data found** vary by breach. Common examples include:

- Email addresses, usernames and display names
- Passwords, including hashed passwords that can sometimes be cracked
- Names, dates of birth and genders
- Phone numbers and physical addresses
- Geographic locations and IP addresses
- Job titles, employers and social media profiles
- Partial credit card data and, in rare cases, government issued identity documents

Passwords deserve immediate attention If a finding lists passwords, treat it as the highest priority. Change that password everywhere it has been used, and switch on multi factor authentication on the affected account.

Sharing your report

Share report link at the top of the report creates a link you can send to a colleague or your IT provider, so they can see the findings without needing access to your AEserver account.

Treat the link as confidential The report lists which of your addresses appear in breaches. Share it only with people who need to act on it.

Get Aman Not monitoring your business yet? See pricing and get started.