Qashew

SAMPLE BRIEF

QASHEW ACCOUNT BRIEF · FOR A SECURITY PLATFORM VENDOR · EMEA

Software group: the lines to open with

Target: **Software group** (two brands) · Seller: **a security platform vendor** · Passive, public records only

1	2	5	0
SIGN-IN TENANT ACROSS TWO BRANDS	CLOUDS, ONE PER BRAND	NON-PRODUCTION AND FILE HOSTS ANSWERING	PACKETS SENT TO THEIR SYSTEMS

- **A real brief, anonymised.** Names, numbers and details changed so the account can't be identified.

THE OPENING LINE

"Both brands sign in through one tenant but run on two clouds. Since the acquisition, who owns identity across the two?"

01 WHAT THE ACCOUNT IS

FACT	VALUE
Business	B2B software. A cloud platform its customers build into their own products through APIs.
Footprint	HQ in Europe. A second brand, acquired a few years ago, with offices in two other European countries.
Ownership	Private-equity owned since early last year.
Scale	Under 200 staff. Carrying significant acquisition debt.
Technology leads	CTO, Information Security Officer and Principal Engineer, all named on the company's own security page. The CEO is a co-founder.
Routing	Direct. An end organisation, with no sign of a reseller or MSSP in the path.

02 VERDICT

Work it. Lead with identity, then AI security, then cloud.

The timing is good. The owner is over a year in, two brands on two clouds are still being joined, and the main product uses AI to score people's work.

WHAT TO SELL

1. **Identity threat protection.** One sign-in tenant holds both brands, and no identity threat tooling is named anywhere.
2. **AI security.** They build and run AI that scores people's work, with accounts at two AI model providers.
3. **Cloud security and exposure management.** Two clouds, with staging and a file-transfer host on the open internet.
4. **SIEM and managed detection and response** follow. Security operations look lean for the size of the customer base.

WHAT IT'S WORTH

Not priced here. At this size, with this much debt, it's a mid-market platform deal. A commit-and-draw-down licence fits: land on identity or AI, then expand as the two estates merge.

03 THE FINDINGS

Three things open the conversation

Each one was read from public records and maps to a line the vendor sells.

One sign-in tenant across two acquired brands RAISE

Both brands' domains resolve to one managed sign-in tenant, registered under the acquired brand's name. Mail for both runs on one provider. Devices are split across two management tools, one for Macs (named as the main platform) and one for Windows. A self-hosted single sign-on answers on two hosts in the first cloud.

Two companies and two clouds are held together by one identity tenant. No identity threat detection is named anywhere public.

Opens: `Identity threat protection`

An AI product that scores people RAISE

The group's own products use AI to score people's work. Domain-verification records for two AI model providers sit in their public DNS, so they hold business accounts with both. Engineering calls itself AI-first and is building agents into the product. When the AI makes the decision, the agent is the product.

This is also where the EU AI Act bites. AI that scores people for decisions about their education or work is a named high-risk use, with the high-risk duties due to apply from December 2027. Their own counsel would confirm the classification.

Opens: **AI security** · runtime protection, shadow AI visibility, AI red teaming

Two clouds and non-production on the open internet RAISE

The home brand runs on one public cloud across several regions. The acquired brand runs on a second cloud, including a US government region. Four staging hosts answer on public cloud addresses, and so does a file-transfer host.

Each brand has its own control plane. There's no sign of one posture view across both.

Opens: **Cloud security and exposure management**

04 WHAT COULD KILL IT

They hold ISO 27001 and a US government cloud certification, so they'll say they're covered. The answer is in section 06. EXPECT

The acquisition debt means every new line of spend gets scrutiny. EXPECT

The strongest single hook, AI scoring of people as high-risk under the EU AI Act, needs their own legal read to confirm. ASK

Nothing public shows what runs on the endpoint for detection, or whether a SOC or managed service sits behind the one named security owner. ASK

Whether the vendor is already in the estate, or across the owner's wider portfolio. ASK, NEVER INFER

Confidence: firm on the estate and the fit. Thinner on in-year budget.

05 WHO TO TALK TO

ROLE	WHY THEM	TALK ABOUT
CTO	Owns the platform and is quoted publicly on security and the government cloud certification. The door for the whole conversation.	Identity, AI security, cloud
Information Security Officer	The named security owner, and the only one public.	Identity threats, SIEM, managed detection and response
Principal Engineer	Named on the security page beside the CTO. Close to how the AI product and both clouds are built.	AI security, cloud posture
CEO and co-founder	The right level for a platform-wide deal, especially with the AI Act angle.	Platform licence, AI Act exposure
Owner's board members	A private-equity owner joining two brands tends to welcome a story that cuts tool sprawl.	Consolidation across both brands

The company publishes role mailboxes only. Approach through the named leaders or a referred introduction.

06 THE FIRST CONVERSATION

WHY CALL NOW

The owner is over a year in, two brands are still being joined across two clouds, and the AI scoring product is growing into EU AI Act scope. An integration is when a platform decision is easiest to make.

QUESTIONS, IN THIS ORDER

Q1 Since the acquisition, who owns identity across the two brands, and across the two clouds?

Q2 When your AI scores someone, what watches the agent and the data it sees?

Q3 What runs on the endpoint today, beyond the two device-management tools?

Q4 Who's on call when something fires at 2am, and what do they watch it in?

Q5 Have your customers started asking for DORA or AI Act evidence yet?

WHEN THEY PUSH BACK

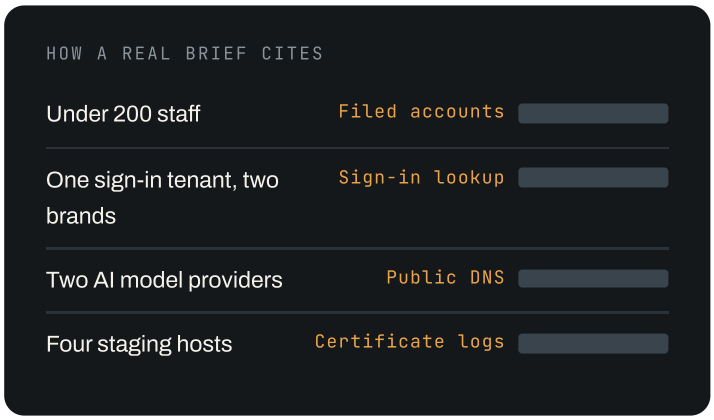
THEY SAY	THE ANSWER
How did you find this?	Public records only: your own pages, company registers, public DNS, certificate logs and your identity provider's public sign-in lookup. Nothing was sent to your systems. An attacker starts in the same place.
We have ISO 27001 and a government cloud certification. We're covered.	Both are real, and both count. They certify a management system and a government baseline. Neither one watches the sign-in tenant for identity attacks, the AI while it scores, or both clouds at once.
We already use our cloud, mail and awareness training providers.	Keep them all. The platform sits alongside them as the detection and response layer across both brands.
Our AI only scores. People make the decisions.	Under the AI Act, scoring people for decisions about their education or work is a named high-risk use. What matters is who can show what the model did, and stop it when it goes wrong. AI security does that, and it's evidence for the Act file.
Budget is tight after the deal.	Commit once and draw down modules as the integration needs them. That beats buying point tools twice across two brands.

07 SOURCES

Every fact in a real brief carries its source and the date it was read: company registers and filed accounts, the company's own pages, public DNS, certificate logs and public sign-in lookups.

In this sample the sources are withheld to protect the account.

Collection is passive. No login, form, port scan or probe of their systems.



Qashew account brief · sample, anonymised · EMEA · routing: direct · passive, public records only