

# Who controls the technology behind a UK retailer?

How much this sector depends on technology suppliers it cannot fully control — and where that matters most.

June 2026

## The big picture

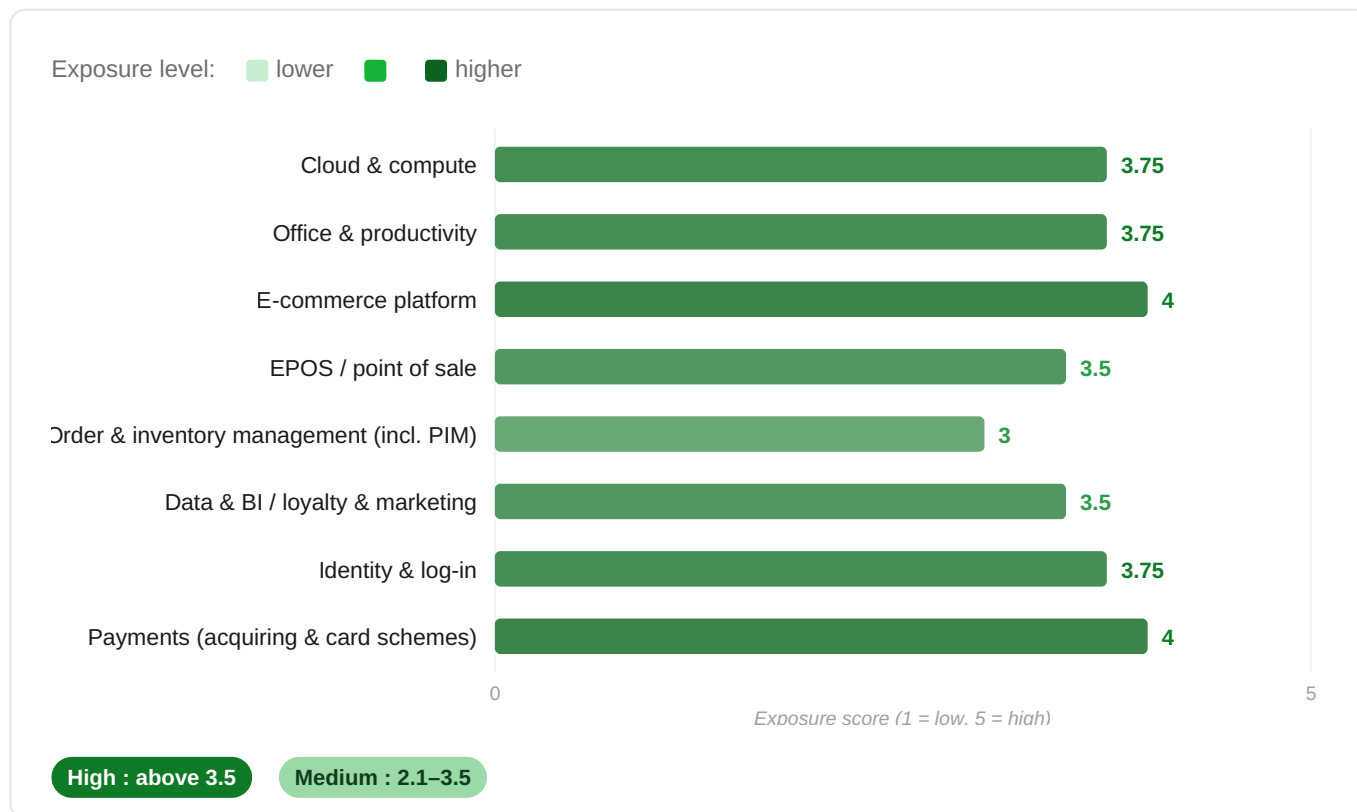
**HIGH EXPOSURE**

**3.6 / 5**

For a typical UK mid-size omnichannel retailer, six of the eight building blocks score High exposure, and they cluster around two foreign-controlled, business-critical layers: the e-commerce platform that runs the website and the payments rail that takes the money. Both are dominated by US (and US card-scheme) suppliers, and payments is the most sensitive and least substitutable of all.

We looked at the everyday layers of technology a UK omnichannel retailer relies on, from the cloud it runs on to the systems that define the sector. A supplier owned in the United States can be compelled to hand over data under US law — the CLOUD Act<sup>[1]</sup>, and the surveillance powers in Section 702 of the Foreign Intelligence Surveillance Act<sup>[2]</sup> — even when that data is stored in Britain; a British supplier answers only to UK law. We scored each building block on four things — how few the suppliers are, whose laws they answer to, how hard they are to switch, and how essential they are.

## Where the exposure sits



## Who controls each layer

The building blocks this sector relies on, coloured by who ultimately controls each one: ■ US-controlled

<b>Cloud &amp; compute</b> Amazon Web Services / Microsoft Azure / Google Cloud	US
<b>Office &amp; productivity</b> Microsoft 365 / Google Workspace	US
<b>E-commerce platform</b> Shopify / Adobe Commerce (Magento) / BigCommerce — UK/EU: Squarespace, Visualsoft, commercetools	US
<b>EPOS / point of sale</b> Shopify POS / Block (Square) / Aptos / NCR Voyix — UK: Epos Now, Citrus-Lime	US
<b>Order &amp; inventory management (incl. PIM)</b> Brightpearl / Linnworks / Cin7 — UK/EU: Brightpearl, Sage, The Access Group, Akeneo (PIM)	US
<b>Data &amp; BI / loyalty &amp; marketing</b> Klaviyo / Intuit Mailchimp — UK: Dotdigital, Eagle Eye, LoyaltyLion	US
<b>Identity &amp; log-in</b> Microsoft Entra / Okta (staff); platform-native customer accounts	US
<b>Payments (acquiring &amp; card schemes)</b> Stripe / Worldpay / PayPal / Block (Square) over Visa & Mastercard — EU/UK: Adyen, SumUp, Teya, Checkout.com	US

*Genuinely UK-controlled options in our data: e-commerce platforms Squarespace, Visualsoft, Tryzens, itim Group; EPOS Epos Now, Citrus-Lime; order/inventory Brightpearl, Sage, The Access Group, K3, Khaos Control; loyalty/marketing Dotdigital, Eagle Eye, LoyaltyLion; open banking TrueLayer; payments Teya. EU-controlled: commercetools (DE), Mirakl (FR), Sana Commerce (NL), ChannelEngine (NL) for platforms; Akeneo (FR), Sales Layer (ES) for PIM; Adyen (NL), SumUp (LU) for payments. None removes the US Visa/Mastercard card-scheme dependency, and several nominally-British products are foreign-owned (Brightpearl's parent group is US-controlled; check ownership before relying on any option).*

## What this means, in plain terms

---

**The defining risk: the shopfront and the till-roll both run on American rails.** Two layers decide whether a retailer can trade at all: the e-commerce platform that runs the website and the payments rail that takes the money. Both are foreign-controlled. The platform market is dominated by Shopify (Canadian-incorporated), Adobe Commerce and BigCommerce (both US); payments runs through US processors such as Stripe, Worldpay and PayPal, and almost every card transaction settles over Visa and Mastercard — both US card schemes. A retailer can change its acquirer but cannot route around the schemes. That is the sharpest, least substitutable dependency on the board<sup>[3]</sup>.

**Payments is the sensitive layer — and it has two faces.** Payments processes cardholder data and the full record of who bought what, when and where — commercially sensitive and regulated (PCI DSS, the Payment Card Industry Data Security Standard). Even where a processor is European on paper, the card schemes that authorise every transaction are American, so the confidentiality and continuity exposure both run back to US-controlled rails. This is the one layer where, unlike a law firm, a retailer is genuinely card-payment-dependent — if it stops, the shop stops<sup>[3]</sup>.

**There are real UK and EU options — but mostly off the critical path.** Genuine UK-controlled e-commerce platforms exist in our data — Squarespace, Visualsoft, Tryzens, itim Group — and EU-controlled headless platforms such as commercetools (Germany), Mirakl (France) and Sana Commerce (Netherlands). In payments, Adyen (Netherlands) and SumUp (Luxembourg) are EU-controlled acquirers, Teya is UK. But none of these removes the Visa/Mastercard scheme dependency, and the largest, best-supported platforms remain American — so the realistic options lower jurisdiction one rung rather than to one.

**Concentration: the platform often pulls payments, POS and identity with it.** Shopify is not one layer — a Shopify retailer typically takes Shopify's platform, Shopify POS, Shopify Payments and Shopify customer accounts as a bundle, so a single Canadian-controlled vendor sits under the website, the till, the checkout and the log-in at once. That correlates the failures: one outage, account action or legal order touches the whole front of the business. Beneath all of it, most platforms and processors run on AWS, Google Cloud or Azure — so the substrate concentrates back onto the same three US clouds.

**The kill-switch test: the website and the till fail in minutes.** If a foreign provider restricted service, the e-commerce platform and the payment rail would fail within hours — the website goes dark, cards stop clearing, and there is no manual workaround at scale. The till has a little more runway in-store (cash, offline modes) but online trade halts. Rebuilding a storefront or re-platforming an acquirer takes months. That gap — fails in hours, fixed in months — is what makes the front-of-business layers the board-level priority.

## If a supplier pulled the plug, how fast would it hurt?

SPEED OF IMPACT	LAYER	WHAT HAPPENS
Hours	Payments (acquiring & card schemes)	Card authorisation stops; online and card-present sales halt. An acquirer can be replaced in weeks–months, but the Visa/Mastercard scheme dependency cannot be routed around at all.
Hours	E-commerce platform	The website goes dark; online trade stops. Re-platforming and migrating the catalogue, orders and integrations is a multi-month project.
Hours–days	Identity & log-in	Customers cannot sign in and staff are locked out of head-office systems; fast failure, but more recoverable than the trading layers.
Days	EPOS / point of sale	In-store tills fail, though cash and offline modes give limited runway; cloud POS degrades fastest.
Days–weeks	Order & inventory management	Stock visibility and fulfilment degrade; workarounds and manual processes buy some time.

## What organisations can do about this

BUILDING BLOCK	PRACTICAL STEPS
<b>E-commerce platform</b>	At the next re-platforming decision, weigh genuinely UK/EU-controlled options against the US incumbents. Our data shows UK-controlled Squarespace, Visualsoft, Tryzens and itim Group, and EU-controlled commercetools (Germany), Mirakl (France) and Sana Commerce (Netherlands). This lowers the jurisdiction one rung (US → 4 to EU → 2–3) and, for a UK supplier, towards 1 — but only at a re-platforming, which is slow and costly, so the renewal is the moment to choose.

---

## Payments

An acquirer can be diversified or moved — EU-controlled Adyen (Netherlands) and SumUp (Luxembourg), or UK-based Teya and Checkout.com, lower the processor's jurisdiction. But no acquirer removes the Visa/Mastercard scheme dependency; account-to-account and open-banking payment routes (TrueLayer is UK-controlled in our data) are the only genuine reduction of card-scheme reliance, and adoption is still early. Treat the scheme dependency as accept-and-monitor.

---

## Order, inventory & loyalty

These back-office layers have the most credible UK/EU choice. Brightpearl, Sage and The Access Group are UK-controlled for order/inventory; Akeneo (France) for PIM; Dotdigital, Eagle Eye and LoyaltyLion are UK-controlled for loyalty and marketing. Preferring these at renewal lowers jurisdiction without touching the critical trading path — the cheapest sovereignty wins.

---

## Cloud, identity & concentration

Avoid taking platform, POS, payments and customer accounts all from one vendor (the Shopify-bundle pattern) — splitting them reduces the single-vendor blast radius even if every part is still foreign. For head-office cloud and staff log-in, UK and European options (OVHcloud, Scaleway, IONOS, the open-source Keycloak self-hosted) reduce reliance on a single US provider.

---

## Data residency & contracts

Where a US platform or processor is unavoidable, insist on UK/EU data residency, UK/EU-law contracting and clear sub-processor disclosure. This lowers the practical blast radius but does not remove US legal reach (the CLOUD Act — the Clarifying Lawful Overseas Use of Data Act 2018 — can compel a US company to hand over data it controls, wherever stored). Document the residual and monitor it.

---

## Sources

---

1. US CLOUD Act 2018 (18 U.S.C. 2713) - compels US-incorporated providers to produce data in their custody wherever in the world it is stored. <https://www.govinfo.gov/content/pkg/USCODE-2018-title18/html/USCODE-2018-title18-partI-chap121-sec2713.htm>
2. US Foreign Intelligence Surveillance Act, Section 702 (50 U.S.C. 1881a) - a US directed-surveillance authority. <https://www.govinfo.gov/app/details/USCODE-2021-title50/USCODE-2021-title50-chap36-subchapVI-sec1881a>
3. Vendor ownership and hosting - taken from company filings, public registries (including UK Companies House) and suppliers' own documentation, compiled in the Information Matters UK vendor sovereignty database.

---

**How we did this.** We scored each technology layer on four things — supplier concentration, whose laws they answer to, how hard they are to switch, and how essential they are — using the IM Sovereignty Framework and our UK vendor database. Control and hosting facts come from primary sources; the harder-to-quantify judgments are our reasoned view of a typical organisation. Scores are bands, not exact measurements. Full evidence record available on request.

This research consists of the opinions of the Information Matters team — human and AI — and should not be considered statements of fact.

*Information Matters* · [informationmatters.net](https://informationmatters.net)

If you have any questions or comments about this article please email [info@informationmatters.net](mailto:info@informationmatters.net)