RED BEAR: ALPHA ENGINE · DATA SHEET · PROTECT · SOVEREIGNTRUST

Your data, your jurisdiction, your control

Three hosting models so residency is a decision you make rather than a limitation you inherit, encryption you hold the keys to, and a documented split of who is responsible for what.

KEY POINTS

- Three hosting models, one application: SaaS in Azure UAE North, Azure Stack Hub in your data centre operated by Red Bear, or containers on your own servers; the data contracts are identical across all three
- Residency is enforced, not advisory: primary storage, processing, backup and every derived artefact stay in the configured region, and an operation that would breach it is blocked and logged
- Customer-managed keys in Azure Key Vault in every model; revoke the key and you revoke our access
- Federated identity through Microsoft Entra ID with multi-factor authentication, so your joiners and leavers govern access, and the platform holds no passwords
- Tenant isolation and authorisation enforced at the API, verified by test; nothing leaves the tenant without clearing a default-deny gateway; every access attributable to a person

What it is

Deal data is confidential, frequently price-sensitive, and often subject to obligations your firm cannot delegate; a firm's own investors may include sovereign wealth funds with strict requirements about where data physically resides. SovereignTrust is how Red Bear: Alpha Engine keeps that data secure and the service available. Across all three hosting models the data itself, the users who may see it and the policy governing access remain yours. What changes between them is how much of the stack beneath that you wish to operate, and how much you would rather we did.

The people who evaluate this pillar are security officers, not investors, and it is why deals get signed or blocked in procurement. For the analyst it means one thing: the tool is approved, so you can actually use it.

The pain point

"It is in a cloud somewhere" ends the conversation. A cloud AI tool is not trusted by default with a data room, and a security review that starts from a brochure runs for months while the deal team works around it. Residency answered late means the mandate's jurisdiction becomes a limitation inherited from the vendor rather than a choice the firm made; encryption the vendor controls means the vendor's access cannot be revoked; and a tool that hides a button instead of enforcing a permission fails the first penetration test.

The answer is to have residency, isolation, encryption and the responsibility split settled before procurement asks, in the jurisdiction the mandate requires, and to be able to evidence them to a CISO rather than describe them.

How it works

Three hosting models. *Model A, software as a service*: Red Bear hosts and operates the product in Azure UAE North, with UAE Central as the paired region; another region only by the tenant's written choice. Fastest to deploy, operating within days; you keep control of your data, users and keys and we run everything beneath them. *Model B, Azure Stack Hub on premises*: we deploy inside your data centre on a platform we manage for you. Your building, your hardware, our platform operations, for firms that cannot place data in a public region. *Model C, containers on your servers*: we supply and maintain the application; you own the infrastructure, the runtime and the operations. The application and its data contracts are identical across all three and the model chosen is recorded per tenant (FR-PROT-001; RBP FR-HO-01, RBP FR-HO-02).

Residency and isolation. The residency region is configured at provisioning and enforced for primary storage, processing, backup and derived artefacts; where the model requires compute to stay local, it stays local (FR-PROT-002). Tenant data is partitioned at the data-access layer and enforced server-side, verified by automated

Encryption and identity. All traffic is encrypted with TLS; where traffic must stay off the public internet, private circuits over Azure ExpressRoute provide layer-2 privacy. Data at rest is encrypted with a platform-managed key or your own customer-managed key in Azure Key Vault, supported in all three models; revoking it removes our access (FR-PROT-005). Users and services authenticate through Microsoft Entra ID with multi-factor authentication, federated to your own directory through Enterprise Applications, so deprovisioning with you removes access with us (FR-PROT-003). Roles (analyst, investment director, partner, operating partner, compliance, administrator) are enforced at the API layer, never only in the interface (FR-PROT-006).

Availability, backup and audit. Azure Site Recovery replicates application and data to a standby site, across availability zones in one city or across a region pair, at your election; the load balancer fails over when the primary becomes unavailable, recovery objectives are agreed per tenant, and failover is tested, not assumed (FR-PROT-008). Encrypted backups are held in regions you nominate under the same residency rule, with point-in-time restore tested on a schedule and

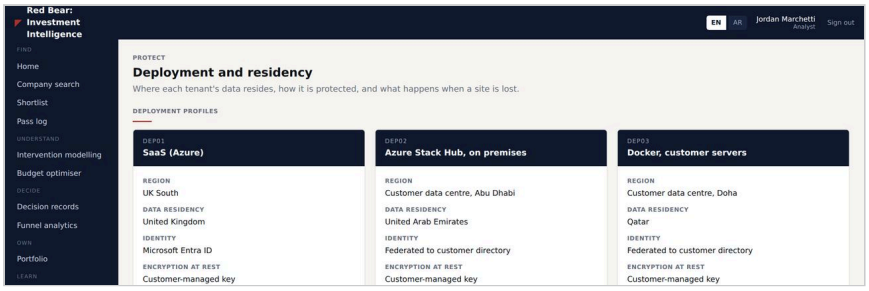
test; cross-tenant attempts are logged and denied (FR-PROT-004; RBP FR-ID-03).

the results available to you (FR-PROT-009). Every data access, model call, override, gateway decision and configuration change is logged with user, time, tenant and outcome, immutably, attributable to a person and never to a service account (FR-PROT-007). Nothing leaves the tenant without passing the Safeguard Gateway, which defaults to deny and cannot be disabled by configuration (FR-PROT-010).

What you get

Capability	What it does	Requirements
Hosting models and data residency	SaaS in Azure UAE North, Azure Stack Hub on premises, or your own servers; residency enforced for storage, processing, backup and derived artefacts	FR-PROT-001, FR-PROT-002
Federated identity and role-based access	Entra ID with MFA, federated to your directory; roles enforced at the API	FR-PROT-003, FR-PROT-006
Tenant isolation	Partition-level isolation enforced server-side and verified by test	FR-PROT-004
Encryption	TLS in transit, ExpressRoute where required; customer-managed keys in Key Vault in every model	FR-PROT-005
Audit logging	Every access, model call, override and change logged immutably to a person	FR-PROT-007
Availability, failover and backup	Active-passive replication across zones or a region pair; encrypted backups in nominated regions, restores tested	FR-PROT-008, FR-PROT-009
Default-deny egress	The Safeguard Gateway on every outbound path, no configuration disables it	FR-PROT-010

Screens



S-12 Deployment & residency: Deployment and residency: the hosting model, region, key ownership, failover topology and gateway posture for the tenant, as the compliance officer sees it. Prototype render on synthetic data for fictional entities.

RETURN ON INVESTMENT

Procurement clears first time. Residency, isolation and encryption are answered before the security review begins rather than negotiated during it. **Regulated and sovereign-adjacent capital is addressable.** The same application deploys into a public region, your own data centre or your own servers without changing its data contracts. **Confidentiality is demonstrable, not asserted.** Tenant isolation, gateway control and audit logging can be evidenced to a CISO. **The evidence trail doubles as a compliance record.** Retaining the material underlying investment recommendations is an obligation the platform satisfies as a side effect of its design. The measure this pillar carries is **time from first security questionnaire to approval to use**, baselined at the first engagement and not given a target here. The control matrix, threat model and responsibility split are available for review under NDA.

Platform engines

SovereignTrust is the product's use of the Red Bear Platform's Identity and tenancy, Audit and Hosting services (RBP FR-ID-01 to RBP FR-ID-04, RBP FR-AU-01, RBP FR-HO-01 to RBP FR-HO-04) and of the AI gateway, which reports per tenant where inference runs and whether that meets the residency requirement (RBP FR-AI-04). Platform behaviour is specified in the platform functional specification, not here.