Jetstone security whitepaper

Security and procurement reviewers

Entity	Black Shard Pty Ltd, ABN 66 696 910 773
Document ID	JET-TRU-07
Pack	Jetstone trust documents library
Prepared for	Security and procurement reviewers
Classification	Public
Version	1.0
Effective date	23 November 2026
Owner	Director

1. Jetstone

Jetstone Business is detection and response for Windows devices and Microsoft 365 and Google Workspace accounts. An agent on each device and a read-only connection to the tenant report to the Jetstone service, which detects attacks, writes up each incident and takes the response actions the workspace's policy allows. People see incidents, approve, dismiss and undo in the console at console.blackshard.com, the desktop app and the phone app.

Jetstone for phones protects a person's own iPhone or Android phone: a web shield, Wi-Fi checks, a device safety check and Scam Check.

Black Shard Pty Ltd builds and runs both. The people who build Jetstone answer its security questions and its vulnerability reports.

2. Hosting and architecture

LAYER	DESIGN
Region	Microsoft Azure, Australia East. An Azure Policy assignment on the production resource group denies any resource outside Australia East
Compute	Azure Container Apps: the console, the agent gateway and the stream processor, plus scheduled jobs. Every container runs from Black Shard's own registry, fixed by image digest, and a second Azure Policy assignment refuses any other image source
Data	Azure Database for PostgreSQL, Azure Blob Storage and Storage Queues, Azure Key Vault Premium, and a language model deployment, each with public network access disabled and reached over private endpoints inside the Jetstone virtual network
Public endpoints	Two: console.blackshard.com for people and agents.blackshard.com for devices, each with an Azure-managed certificate
Identity between services	Each app and job runs under its own managed identity, with Key Vault access granted secret by secret. No secret sits in an app's configuration

3. Encryption

CONTROL	HOW JETSTONE APPLIES IT
In transit	TLS 1.2 or 1.3 on every public endpoint; older versions are refused. The console sends Strict-Transport-Security for two years, including subdomains. PostgreSQL requires TLS 1.2 or later
At rest	Every data store is encrypted at rest. Storage accepts Entra authorisation only, with shared key access disabled and no public blob access
Keys	The device certificate authority key and the command envelope key are hardware security module keys in Key Vault Premium, usable to sign and never exported. Only the agent gateway's identity can use them. Purge protection is on and deleted keys are held 90 days

4. Device trust

- Each enrolled device holds its own certificate, issued by Jetstone's device certificate authority, and proves it on every connection. The gateway checks the chain, expiry, revocation and the device's binding to its workspace before accepting any data.
- Commands to a device are signed envelopes, bound to that device and checked for replay and expiry. The guardrails are checked again at the moment a command is dispatched.
- The agent is a signed user-mode service. It installs an update only when the signature verifies against the key built into it.
- Removing the agent through Windows needs the device's uninstall code, which an owner or administrator reveals in the console.
- Each phone running Jetstone signs its requests with a key held in its secure hardware, confirmed with Apple or Google attestation. The lists and settings a phone downloads are signed, and the app refuses one older than the last it accepted.

5. Access to the console

CONTROL	DESIGN
Sign-in	Passkey, Sign in with Microsoft or Google, or a one-time code sent by email. No passwords. A workspace can require a passkey or single sign-on for every member
High-impact changes	Isolating a device, reversing containment and moving the policy to Watch each need a passkey, or the desktop or phone app's hardware approval key, signing the exact change. The service checks that signature twice, at the console and again at the gateway, before anything changes
Other changes	A step-up no older than five minutes
Sessions	Idle and absolute session limits, rate limits on sign-in, single-use signed links for approve and undo, every other session ended on account recovery
Roles	Owner, administrator and viewer. The owner invites each person, and a move to Watch or the loss of an owner emails every owner
Browser protection	A strict Content Security Policy with per-request nonces, framing denied, every device feature denied except passkeys

6. Workspace separation

Each workspace's records carry its workspace identifier, and PostgreSQL row-level security enforces the boundary under an application role that cannot bypass it. Storage paths carry a workspace prefix and every storage link is minted for one workspace. A cross-workspace property test covers every list endpoint and every storage link mint, and a request for another workspace's record answers as if the record does not exist.

7. Tamper evidence and monitoring

- Audit records are hash chained. A scheduled job verifies every chain daily and alerts on any break.
- Raw device telemetry is held under time-based immutability for 12 months, locked so that no identity, an owner included, can shorten or remove it.
- Activity log alerts fire on any change to role assignments, resource locks, workload identity federation, data plane configuration, the activity log export and the alert rules themselves.
- Health, restart and replica alerts cover each app, and every scheduled job has a failure alert.
- Key Vault audit events and PostgreSQL logs, with data definition and role changes audited, go to a Log Analytics workspace kept for 90 days.
- Microsoft Defender for Cloud covers the Jetstone storage account, key vaults and database server.

8. Resilience and backup

CONTROL	DESIGN
Database	Point-in-time restore over 35 days, with geo-redundant backups copied to Azure Australia Southeast, the paired Australian region
Restore	The restore runbook is exercised on production: a restore to a new server, every table's row count and content hash compared before any connection moves
Telemetry	Immutable for 12 months; deleted blobs and containers recoverable for 30 days
Deletion protection	Resource locks on every production data resource, with an alert on any lock removal
Devices	The agent keeps its local rules and up to 72 hours of telemetry while a device is offline

9. Secure development and release

- Every change reaches main through a pull request with seven required checks (Rust, console, lint, mobile, Android, desktop and dependency checks) and resolved review conversations. The rules apply to administrators too, and force pushes and branch deletion are blocked.
- Secret scanning with push protection, dependency alerts with automatic security updates, and copy and claims checks run on every change.
- Every container image is scanned before it is pushed, fails on a fixable critical vulnerability and ships with a software bill of materials.
- Deploys authenticate to Azure with short-lived workload identity federation, scoped to the production resource group, and roll images by digest. No long-lived cloud credential is stored on a build runner.
- Signing keys stay in hardware security modules and secret stores outside the build runners. Customer builds must pass a signature gate that checks the publisher is exactly Black Shard Pty Ltd.

10. Black Shard's own operations

- Every account uses phishing-resistant multi-factor authentication, and admin access is granted just in time.
- Sign-in from outside Australia and legacy authentication are blocked for staff accounts.
- Build hosts run endpoint detection and response, unattended security patching and full command auditing.
- Black Shard Pty Ltd holds SMB1001:2026 Gold, issued by CyberCert, valid 16 June 2026 to 17 June 2027.
- Essential Eight Maturity Level 3, assessed September 2026.

11. Privacy

Jetstone is run under the Privacy Act 1988 (Cth) and the Australian Privacy Principles. Black Shard does not sell personal information and does not use it to train models. Incident write-ups are produced by a language model deployment in Black Shard's own Azure subscription in Australia East, from a redacted evidence pack.

On phones, the sites a person visits and the networks they join are checked on the phone and stay there. A message sent to Scam Check is read once for that check and is not kept.

In Jetstone Business, the agent does not read file contents, email bodies or documents, and command lines and script text are filtered on the device for credential patterns before they are sent. Quarantined files stay on the device that quarantined them.

The privacy notices are at blackshard.com.au/legal/jetstone.

12. Incidents and vulnerability reports

Black Shard tells the customer without undue delay, and in any case within 72 hours, after becoming aware of a breach affecting customer data, and helps the customer meet its own obligations under the Notifiable Data Breaches scheme.

VULNERABILITY REPORT STEP	TARGET
Acknowledge	Within 2 business days
Confirm or rule out, with a severity	Within 5 business days
Update until fixed	At least every 10 business days
Fix a critical finding	Within 7 days

Research that follows the published disclosure policy at blackshard.com.au/trust/security is authorised by Black Shard. The security contact is in /.well-known/security.txt.

13. Sub-processors

SUB-PROCESSOR	PURPOSE	LOCATION
Microsoft Corporation (Azure)	Hosting, storage, the incident write-up model	Australia East
Microsoft Corporation (Microsoft 365, Black Shard's tenant)	Sign-in codes and notices by email	Australia
Cloudflare, Inc.	DNS, the public site and update delivery; no workspace data	Global edge network
Stripe, Inc.	Billing	United States
Apple Inc. and Google LLC	Push notifications carrying an opaque id; phone attestation; store purchases	United States and other locations

Black Shard gives Business customers 30 days' notice by email before adding or replacing a sub-processor.

14. Contact

Security questions: info@blackshard.com.au. Service status: blackshard.com.au/trust/status.