



SECURITY & TRUST

Security & Trust Overview

Synthrics hosts all customer data in Australia, keeps every customer in its own isolated database schema, storage container and search index, and signs users in through your own Microsoft Entra ID.

For IT, security, legal and procurement teams

October 2026 · Synthrics Pty Ltd · ABN 34 692 474 696

ABOUT THIS DOCUMENT

How Synthrics protects your data

Synthrics hosts all customer data in Australia, keeps every customer in its own isolated database schema, storage container and search index, and signs users in through your own Microsoft Entra ID.

This overview is written for the IT, security, legal and procurement teams reviewing Synthrics as a supplier. It covers how the platform is built and run, how customer data is protected, and the commitments we make.

It is a summary, not a security questionnaire. If you need more detail for a vendor assessment, contact us using the details at the end of this document.

AT A GLANCE

Hosted in Australia Customer data, backups and logs are stored in Azure data centres in Australia.	Isolated per customer Every tenant has its own database schema, storage container and search index.
Your sign-in, your policies Users sign in with Microsoft Entra ID, so your MFA and Conditional Access apply.	Not used to train AI Your content is never used to train AI models, by Synthrics or our AI providers.

CONTENTS

01	Executive summary	3
02	Security architecture	4
03	Data protection	5
04	Identity and access management	7
05	Secure development	8
06	Monitoring and incident response	8
07	Operational security	9
08	Business continuity	9
09	Compliance and privacy	10
10	Security FAQ	11
11	Security contact and responsible disclosure	13

01 Executive summary

Synthrics is a multi-tenant SaaS platform that uses AI to process bid, tender and procurement documents.

Customers upload tender packs, and the platform classifies documents, extracts requirements and questions, produces summaries and supports response drafting grounded in the customer's own content.

Platform model. Synthrics runs as a single cloud service on Microsoft Azure in the Australia East region. All customers use the same application, but each customer (a "tenant") has its own database schema, storage container and search index. The application enforces tenant boundaries on every request, using identity taken from a verified sign-in token and never from anything the browser supplies.

Security approach. We build on managed Azure services so that we inherit Microsoft's physical, platform and infrastructure controls. On top of that we apply defence in depth: an edge web application firewall, private networking for data services, encryption everywhere, least-privilege access and continuous monitoring. Infrastructure is defined as code, peer reviewed and deployed through automated pipelines.

Shared responsibility. Security is shared between Synthrics, our cloud providers and you.

Area	Synthrics	Your organisation	Cloud providers (Microsoft, AWS)
Physical data centres, hardware, host infrastructure	—	—	• Responsible
Application security, tenant isolation, encryption, backups	• Responsible	—	◦ Supporting
Network protection, monitoring, incident response for the platform	• Responsible	—	◦ Supporting
User sign-in, MFA and Conditional Access policies	Validates tokens from your directory	• Responsible (configured in your Entra ID)	—
Who is invited and which roles they hold	Provides role-based access controls	• Responsible	—
Content uploaded and how it is classified and shared	Protects and processes it	• Responsible (data owner)	—
Users' devices and networks	—	• Responsible	—

02 Security architecture

All customer traffic enters through a single protected edge, and data services are reachable only from inside the platform's private network.

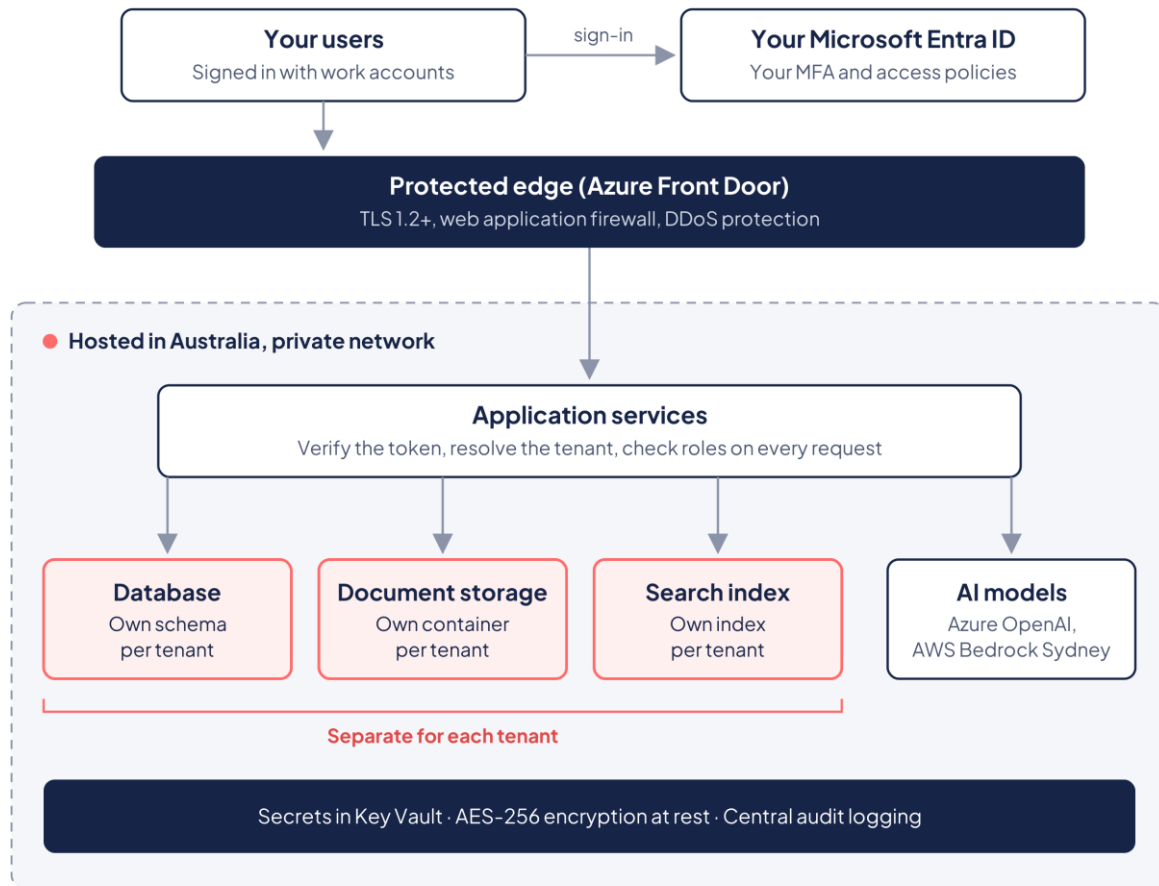


FIGURE 1 Synthrics platform at a high level. Users reach the platform only through the protected edge. Data services have no public access, and each tenant's data sits in its own schema, container and index.

Hosting. Microsoft Azure, Australia East region, using managed platform services wherever possible. The application runs as stateless containers on a managed Kubernetes service that scales horizontally.

Edge protection. Azure Front Door terminates TLS and applies a web application firewall in prevention mode, DDoS protection and bot mitigation before any request reaches the application.

Private networking. The database, document storage, search and key management services are connected through private endpoints and have no public network access. Network security rules allow only the traffic each component needs.

Network segmentation. Development, staging and production run in separate environments with separate cloud subscriptions, networks and identities. Shared management services sit in a hub network apart from application workloads.

Service-to-service security. Internal services authenticate each other with signed tokens and managed identities rather than stored passwords. Internal-only interfaces are blocked from external access by policy.

Multi-tenant model. One deployment serves all customers. Tenant isolation is enforced at the data layer and in the application on every request (see section 3).

High availability and recovery. Services are deployed across Azure availability zones in Australia East. Because the whole environment is defined in code, it can be rebuilt in Australia Southeast if a full regional outage required it (see section 8).

03 Data protection

Customer data is encrypted in transit and at rest, stored only in Australia, and separated per tenant at every storage layer.

Encryption

In transit. TLS 1.2 or higher on every public endpoint (TLS 1.3 where supported), with HTTP Strict Transport Security. Connections between internal services and to the database are also encrypted.

At rest. Databases, document storage, search indexes and backups are encrypted with AES-256 using Azure platform encryption.

Key management. Encryption keys are managed by Microsoft through Azure's key management service, including rotation. Application secrets and signing keys are held in Azure Key Vault, accessed by managed identity, and never stored in source code. Customer-managed keys can be offered with a dedicated deployment.

Data residency

- Customer data, including uploaded documents, extracted content, search indexes, backups and logs, is stored in Azure data centres in Australia.
- AI processing runs on Microsoft Azure and Amazon Web Services AI services configured to process data in Australian regions. Cross-region inference options that could route data overseas are disabled.
- Synthrics staff and contractors may access the platform from outside Australia to provide support and operate the service. This access is controlled as described in sections 4 and 7, and customer data does not leave Australian storage as a result.

Tenant isolation

Each tenant receives its own isolated resources when it is onboarded:

Layer	How tenants are separated
Database	A dedicated PostgreSQL schema per tenant, accessed through a database role that can only reach that schema
Document storage	A dedicated storage container per tenant. Uploads and downloads use short-lived access links (30 minutes or less) issued by the server and scoped to that tenant only
Search and AI retrieval	A dedicated search index per tenant. AI-generated content is grounded only in the requesting tenant's index
Application	Tenant identity comes from the verified sign-in token. Tenant identifiers supplied by the browser are never trusted, and requests without a resolvable tenant are denied
Caching and observability	Cache keys and AI tracing data are scoped per tenant

There is no administrative mode in production that bypasses tenant boundaries. Customers with stricter requirements can discuss a dedicated single-tenant deployment.

Uploaded files

New uploads are held as untrusted and scanned for malware before they are processed. Files that fail scanning are not processed.

AI and your data

- Your content is used only to provide the service to you. It is not used to train AI models, by Synthrics or by our AI providers.
- AI prompts keep system instructions separate from document content, and responses are grounded in your own documents. The AI does not browse the web.
- Provider content safety filters and our own input and output checks help defend against prompt injection and harmful output.

Backups

- The database is backed up continuously with point-in-time recovery, retained for 35 days.
- Document storage uses soft delete and versioning, so deleted or overwritten files can be recovered for 30 days.
- Search indexes can be fully rebuilt from source data.
- All backups are encrypted and remain in Australia.

04 Identity and access management

Users sign in with their existing Microsoft Entra ID work accounts, so your organisation's identity policies apply to Synthrics automatically.

Single sign-on. Sign-in uses Microsoft Entra ID with OpenID Connect. Your Entra administrator grants consent once during onboarding, and users from directories that have not been onboarded are refused. If your Entra ID tenant federates with another identity provider, that setup continues to work. Direct sign-in with other identity providers is not currently offered.

No local passwords. Synthrics does not create or store user passwords, so password policy, account lockout and lifecycle are governed by your directory.

Multi-factor authentication. MFA and Conditional Access are enforced by your Entra ID policies, including device, location and risk-based rules.

Role-based access control. Access within a tenant is governed by roles at workspace and project level (for example Workspace Admin, Manager, Member, Bid Manager and approver roles). Permissions are checked server-side on every request, and list results are filtered to what the user is allowed to see.

Least privilege. New users receive only the roles they are invited with. Workspace administrators control invitations and role changes, and invitation links are single-use and expire.

Sessions. The platform does not issue its own session cookies. Short-lived access tokens issued by Entra ID (typically 60 to 90 minutes) are refreshed silently and held only in browser session storage, which is cleared when the tab closes. Disabling a user in your directory stops new tokens being issued.

API security. Every API call requires a valid bearer token whose signature, audience and expiry are verified. Requests are validated against strict schemas and rate limited per tenant.

05 Secure development

Every change to the platform, including infrastructure, is peer reviewed and passes automated security checks before it can be deployed.

Secure SDLC. Security requirements, tenant isolation and threat scenarios are considered at design time and recorded in architecture decision records.

Code review. All changes go through pull requests with mandatory peer review and protected main branches. Direct changes to production are not permitted.

Automated security scanning. Continuous integration pipelines run static code analysis, dependency vulnerability scanning, secret detection, container image scanning and infrastructure-as-code checks. Findings are triaged and fixed by severity.

Dependency management. Third-party dependencies are monitored continuously and updated through reviewed pull requests.

Infrastructure as code. Cloud infrastructure is defined in version-controlled code, so every change is reviewed, auditable and repeatable.

Change management. Releases are promoted through separate development and staging environments before production, and every release is tagged and recorded. Staging mirrors production security policies.

Penetration testing. Independent penetration testing, with tenant isolation as a primary objective, is planned ahead of general availability. A summary of results will be available under NDA once testing is complete.

06 Monitoring and incident response

Security and operational events are logged centrally, monitored continuously and escalated through a documented incident response process.

Security logging. Application, infrastructure, firewall and access logs are collected in a central log platform within Australia. Every API request is logged with tenant and user context, and audit logs are retained for at least 180 days.

Threat detection. Microsoft Defender for Cloud and Defender for Storage provide threat detection across cloud resources and uploaded content.

Alerting. Alerts cover authentication anomalies, privilege and role changes, failed tenant resolution, unusual data access, rate limit breaches, service health and certificate expiry. Alerts are routed to the engineering team for triage.

Incident response. Incidents are triaged by severity, contained, investigated and resolved under a documented process, followed by a post-incident review and corrective actions.

Customer notification. If an incident affects your data, we will notify your nominated contacts without undue delay and within the timeframe in your agreement. Notifications include what happened, the data involved, the actions we have taken and what we recommend. We also meet our obligations under the Australian Notifiable Data Breaches scheme and the New Zealand Privacy Act 2020.

07 Operational security

Synthrics staff and contractors work only from managed, monitored environments, and access to production is limited to the people who need it.

Managed work environments. Engineers, including contractors, work from company-managed Azure cloud PCs. Access to Synthrics systems is restricted to those managed environments, so source code and platform access never sit on personal devices.

Device security. Any device used to reach Synthrics environments must be enrolled in Microsoft Intune, with full-disk encryption, active endpoint protection and current patches.

Employee access controls. MFA is mandatory for all staff access to cloud environments, source code and collaboration tools. Access is role-based, granted on a least-privilege basis, logged to named individuals and removed promptly when no longer needed.

Production data access. Staff do not access customer content in the normal course of operations. Access for support or incident response is limited to authorised engineers and is logged.

Personnel. Staff and contractors are bound by confidentiality obligations and acknowledge our security requirements before receiving access. Security awareness training is provided at onboarding and refreshed periodically.

Vendor management. Suppliers that may process customer data are assessed for security and data residency before use and reviewed periodically. Current subprocessors are listed in section 9.

08 Business continuity

The platform is designed to survive the loss of a data centre within Australia East and can be rebuilt from code and backups if a wider failure occurs.

High availability. Application services run as multiple replicas spread across Azure availability zones, with automatic scaling and self-healing. Managed data services provide built-in redundancy within the region.

Backups. Continuous database backups with point-in-time recovery, 30-day recovery of deleted or overwritten documents, and search indexes that can be rebuilt from source data (see section 3).

Disaster recovery. Infrastructure is defined entirely in code. If Australia East became unavailable for an extended period, we would rebuild the platform in Azure Australia Southeast and restore data from backups, keeping data within Australia.

Recovery readiness. Restore and rebuild procedures are documented in runbooks.

Service status. Public endpoints, internal services, certificates and critical dependencies are monitored around the clock, with alerts to the engineering team.

09 Compliance and privacy

Synthrics is designed to meet Australian and New Zealand privacy law, and our controls are aligned with ISO/IEC 27001:2022 and SOC 2 principles.

Synthrics does not currently hold ISO 27001 certification or a SOC 2 report.

Frameworks and laws

Framework	Position
Australian Privacy Act 1988 and Australian Privacy Principles	Designed to support compliance. Privacy by design, data minimisation and Australian data residency are core principles
Notifiable Data Breaches scheme (Australia)	Breach assessment and notification process in place
New Zealand Privacy Act 2020	Designed to support compliance, including notifiable privacy breaches
GDPR	Controls support customers' GDPR obligations where they apply. Data is not stored in the EU
ISO/IEC 27001:2022	Controls aligned with ISO 27001 principles. Not certified
SOC 2	Controls mapped to the SOC 2 Trust Services Criteria. No SOC 2 report has been issued
Cloud providers	Microsoft Azure and AWS hold ISO 27001, SOC 2 and IRAP assessments for the services we use

Data ownership and use

- You own your data. Synthrics processes it only to provide and support the service, under your instructions.
- We do not sell customer data, and we do not use it to train AI models.
- A Data Processing Addendum can be agreed as part of contracting.

Subprocessors

Subprocessor	Purpose	Data location
Microsoft Azure	Hosting, storage, databases, search, document intelligence, AI models, transactional email	Australia
Amazon Web Services (Bedrock)	AI model inference	Australia (Sydney)

We will notify customers before adding a subprocessor that processes customer data.

Retention and deletion

- Customer content is retained for the life of your subscription, and you can delete documents and projects at any time.
- When a subscription ends, your tenant's database schema, storage container and search index are deleted. Residual copies in backups expire on their normal retention cycle.
- Written confirmation of deletion is available on request.

10 Security FAQ

Do you support Microsoft Entra ID single sign-on?

Yes. Entra ID is how all users sign in. Your administrator grants consent once, and your MFA and Conditional Access policies apply.

Can we enforce MFA?

Yes, through your own Entra ID Conditional Access policies. Synthrics does not hold passwords, so it cannot weaken them.

Where is our data stored?

In Microsoft Azure data centres in Australia. AI processing uses Australian regions of Microsoft Azure and AWS.

Is our data encrypted?	Yes. TLS 1.2 or higher in transit and AES-256 at rest, including backups.
How do you keep our data separate from other customers?	Each customer has its own database schema, storage container and search index. Every request is checked against the tenant in the user's verified sign-in token.
Is our data used to train AI models?	No. Neither Synthrics nor our AI providers use your content for training.
Who at Synthrics can see our documents?	Staff do not access customer content in normal operations. Limited, logged access is used only for support you request or for incident response.
What happens if there is a breach?	We notify your nominated contacts without undue delay, within the timeframe in your agreement, and meet our notification obligations under Australian and New Zealand law.
Can we get our data back, and is it deleted when we leave?	You can download your uploaded documents at any time. When your subscription ends, your tenant's data is deleted and backup copies expire on their normal cycle.
Which subprocessors do you use?	Microsoft Azure and Amazon Web Services, both processing data in Australia. See section 9.
Are you ISO 27001 certified or SOC 2 audited?	Not yet. Our controls are aligned with ISO 27001 and mapped to SOC 2, and we run on providers that hold both.
Can we run a penetration test or security review?	Yes, by arrangement. Contact us to agree scope and timing.

11 Security contact and responsible disclosure

SECURITY CONTACT

security@synthrics.com

Send security questions, assessment requests and vulnerability reports to this address.

2 business days
to acknowledge a
vulnerability report

Reporting a vulnerability. If you believe you have found a security issue in Synthrics, please email us with a description, the steps to reproduce it and any supporting evidence. We will acknowledge your report within 2 business days, keep you updated while we investigate, and let you know when it is resolved.

Our commitments to researchers. We will not take legal action against good-faith research that follows these guidelines:

- Only test against accounts and data you own.
- Do not access, change or delete other customers' data.
- Do not degrade the service, for example through denial-of-service or automated high-volume testing.
- Give us reasonable time to fix the issue before disclosing it publicly.

Vendor assessments. We can provide further detail, complete security questionnaires and share supporting documents under NDA as part of your procurement process.

Synthrics Pty Ltd · ABN 34 692 474 696. This overview describes the Synthrics platform as at October 2026.