

How Theodolite handles your data

A practical guide to deployment, data storage, access and security review

SECURITY OVERVIEW

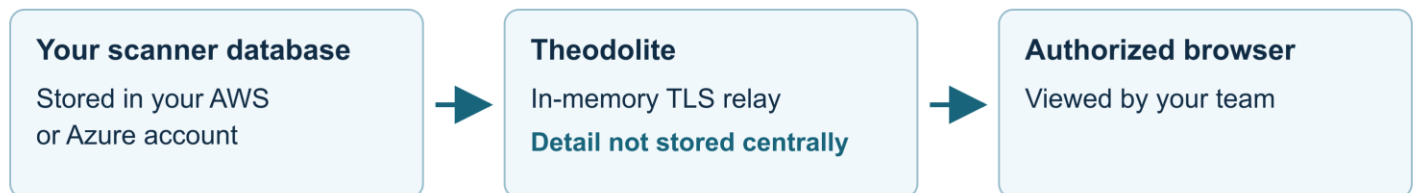
Theodolite helps your team review cyber exposure in supported cloud and SaaS environments. Your scanner and its findings database run in your own AWS or Azure account. This guide explains what stays there, what moves through Theodolite, and what we store to operate the service.

1 The picture at a glance

There are two data paths. Detailed records are stored in your scanner database and relayed when an authorized user opens them. Scan activity and permitted measures are sent to Theodolite and stored centrally.

Detailed records

Stored in your cloud and relayed for authorized viewing



Scan activity and permitted measures

A separate path to central storage



When your team opens a finding: the result travels from your scanner through Theodolite in memory over an encrypted connection to the requesting browser. Theodolite does not store that detailed result centrally. The result does pass through our service; it is not a direct scanner-to-browser connection.

When your scanner reports progress: Theodolite stores operational information such as run status, timing and permitted result totals. These records help the service show scan activity and available measures.

Your scanner can assess only the sources its permissions allow it to read. SharePoint requires a separate connection and authorization. Missing access, incomplete reads and partial scans limit what the results can establish.



2 What is stored and where

In your cloud account

Detailed findings, inventory, access evidence and file-processing diagnostics are stored in your scanner database. Source-connector secrets are kept in your own Azure Key Vault or AWS Secrets Manager.

You select a supported deployment location for your scanner. Theodolite's central application, API and database are hosted on Microsoft Azure in Central US. Customers cannot currently select a different central hosting region.

In Theodolite central storage

Record category	What it includes
Runtime and scan telemetry	Scanner status, last check-in, reported software version and deployment identifiers. Run, source and account identifiers; completion or partial status; start and end times; errors.
Observed resource totals	Counts of subscriptions, resources, storage accounts, databases and compute. Counts of storage observed as public or unencrypted.
Derived security measures when available	Security-check pass and fail totals; sensitive-data indicator and affected-location count ranges; coverage and known limitations; vulnerability presence, severity and coverage.
Conditional risk records	For organizations where the computation is enabled and has generated results, the resulting risk figures and their basis are retained centrally. This does not mean every customer has a risk estimate.
Service and access records	Account, organization and scanner registration; sign-in and authentication records; submitted contact and partner requests; privileged-access audit records including actor, target, times and recorded IP address.

These measures describe security posture rather than file contents. They can still be sensitive information about your organization; "summary" does not mean anonymous.

A separate installation exception

Azure Portal setup temporarily places protected deployment files in Theodolite-managed storage. Some contain credentials needed to install the scanner. That handling is separate from the customer-held source-connector secrets described above. The next page explains the protection and cleanup boundary.

3 Access and safeguards

Permissions follow the task

Source scanning reads the customer sources you authorize. Installation also needs permission to create and manage the scanner's own infrastructure. Some lifecycle permissions can manage that infrastructure, so the complete deployment permission set is broader than source-read permissions.

Review the exact grants for your chosen cloud and deployment route. Additional accounts or subscriptions need their own authorized scope; installing one scanner does not automatically authorize an entire organization. SharePoint access is authorized separately.

Source secrets and protected setup

Source-connector secrets live in your cloud's Key Vault or Secrets Manager. During Azure Portal installation, three setup files are staged in private, restricted Azure Blob storage. They include deployment and launch instructions, plus parameters containing scanner setup and signing credentials, registry-pull credentials and the scanner database password.

Read-only links to these files expire within two hours. Link expiry limits access and is separate from file deletion. Cleanup is attempted after connection, expiry or offboarding, and failures are recorded and retried. A fixed removal deadline is not guaranteed. Review any required cleanup escalation or notification commitment with us before deployment.

Sign in and support access

Customer sign-in uses Microsoft authentication. Multifactor authentication follows your organization's Microsoft identity policy. It should not be assumed to be a separate Theodolite-enforced requirement for every customer sign-in. Application sessions have a 30-minute idle timeout.

Everyday application access is scoped to your organization. Privileged support access uses a named administrator identity tied to a specific target; the grant and its use are audited. Internal administration also requires a one-time password in addition to the administrator's login credentials.

Encryption

The central application and API require HTTPS with TLS 1.2 or later. The central database encrypts data at rest with Azure-managed keys. Encryption settings for resources in your own cloud account depend on their configuration.



4 Retention and security review

Offboarding and deletion are separate

Offboarding revokes scanner access to the service and retires registry credentials. It does not automatically delete central organization, run or risk records. Do not treat the end of a connection as confirmation that all related records have been removed.

Before deployment, agree the retention and deletion requirements for each data category, including backups, logs, audit records and any legal hold. Backup recovery windows and infrastructure-log retention periods do not determine how long active service records are retained. The scanner database in your own account also needs an explicit retention and disposal plan.

Evidence for your review

You can request architecture and data-flow documentation and a deployment-specific security review. Further detail can be discussed under NDA. Ask about the current evidence available for any independent assurance requirement and the scope it covers.

Use the review to resolve requirements that depend on your deployment and agreement:

- The exact source permissions and scanner hosting location.
- Access to your organization, privileged support and audit-record retention.
- Central record retention, deletion requests, backups and holds.
- External service providers, their roles and the applicable contractual disclosures.
- Protected setup-file cleanup and escalation requirements.
- Incident contacts, notification obligations and the applicable response process.

Questions or a vulnerability to report

Use the security-review contact form for a security concern or vulnerability report. Confirm any required response times and reporting arrangements with us during your review.

[Request a security review or report a concern](#)

[Read the online Trust Center](#)

[Review AWS and Azure deployment guidance](#)

[Read the privacy policy](#) and [terms of service](#)

This guide explains the product's data handling. Confirm deployment-specific requirements and contractual commitments with Theodolite before relying on them.