Atmoz Setup, Security and Data Governance

Mar 2026

About Atmoz

Atmoz is a real-time, Azure-native SaaS platform designed to help organizations eliminate cloud waste before it happens. We deliver instant, actionable insights into resource usage, costs, and inefficiencies, right where your teams work - so they can make informed decisions in the moment, to eliminate waste.

By combining read-only, secure access with advanced telemetry analytics, Atmoz empowers engineering, DevOps, and FinOps teams to:

- Gain full visibility into resource configurations, costs, and ownership across subscriptions and regions.
- Detect and prevent inefficiencies such as unused or orphaned resources before they impact your budget.
- Receive targeted recommendations directly in Microsoft Teams, Slack or email, ensuring the right people take the right action, quickly.

Because Atmoz never requires write access, your teams remain in full control of all changes, while benefiting from a secure, compliant, and Azure-native solution built for enterprise governance needs.

For more information, please visit www.atmoz.co.

Purpose of this document

This guide outlines Atmoz's approach to security, data handling, and governance as a SaaS platform for Azure cost optimization and telemetry analytics. It's designed to answer common questions from security and governance teams prior to onboarding.

For further questions, please email support@atmoz.co or request a meeting.

Table of Contents

Quick, Secure Setup and Access

Setting up Atmoz is easy - a 30-second process, plus a 3–4-minute provisioning time. No complex configuration required.

Installation is handled via one click in the Azure Marketplace to set up Atmoz, Teams app Marketplace to set up Finius, Atmoz Portal or the Chrome Extension. The Azure Marketplace installation provides access to the Atmoz platform, that oversees and optimizes your resource usage. The extension provides full visibility of the Azure resources and prices across regions and zones – even those which you do not currently use.

Atmoz connects to Azure using the following read-only permissions:

- Subscription Reader
- Subscription Monitoring Reader
- Subscription Billing Reader

You can scope these permissions to a subscription or resource group as preferred, per resource group, per subscription. If you have any questions or need any support, please contact Atmoz at support@atmoz.co.

All optimizations are recommended only - Atmoz never acts automatically; humans remain in full control.

Onboarding Steps

When you log in to portal.atmoz.co for the first time, you will be guided through the two steps above. The explanations provided here are for your reference. You can also perform these steps manually if you prefer.

Note: Atmoz uses Azure's Single Sign-On (SSO) for a secure and seamless login experience.

Permissions

Atmoz is a fully Azure-native platform, hosted and processed within Microsoft Azure,

using secure APIs and services. Access is primarily managed through Azure Lighthouse or Azure Active Directory Service Principal, per your preference, providing robust enterprise security and control.

- All connections use Microsoft's secure identity platform; no generic or personal accounts.
- All API access is authenticated and authorized
- No external subcontractors or third-party processors handle your data

Extra Permissions

For automatic resource owner assignment and user notifications, the User.Read.All permission is needed. Admins can grant this securely via Azure. If this permission is not granted, Atmoz will only be able to retrieve user information when users log in.

To grant this permission, please approve admin consent using the following URL (replace {tenantId} with your Azure tenant ID): https://login.microsoftonline.com/{tenantId}/adminconsent?client_id=69079be5-353f-4001-9b09-c4ccb6387655

Bot Installation - Finius:

- Atmoz Teams Bot: Install from Microsoft Teams App Store
- Atmoz Slack Bot: Install from Slack App Directory

This ensures proactive, targeted communication with relevant users only when necessary.

Data Handling & Classification

Atmoz analyzes Azure data to:

- Generate real-time cost optimization insights
- Detect inefficiencies, unused, or orphaned resources
- Provide actionable recommendations delivered via Teams or Slack bots

What Atmoz Collects

Atmoz connects to Azure using read-only roles to access:

- Resource metadata: types, configurations, tags, usage metrics
- Operational telemetry: activity logs, resource events
- Billing data: cost and usage records

Atmoz Does NOT Access:

- Customer application data
- Content/data within workloads, databases, or files
- Personal data, secrets, or sensitive production information
- Cardholder Data Environment (CDE) or cardholder data

For example:

- *On a Virtual Machine scale set (VMSS), we only see the capacity, the Virtual Machine (VM) type, and the VM scale set name.*
- *You can run a query such as 'resources | take 1' in the Azure Resource Graph Explorer to see the type of data Atmoz collects.*

Atmoz tracks its own infrastructure changes for service integrity, plus customer metadata events for cost impact analysis only.

As mentioned, optimizations are recommendations only and humans always approve changes.

Sensitive Data Handling

Since naming can sometimes include sensitive information, like your customer or project names, Atmoz encrypts any names within our database, including resource names and any user details.

Each customer (tenant) has a unique, separate encryption key, which is kept under a secure Azure key vault service.

PCI DSS and Cardholder Data Environment (CDE)

Atmoz does not process, read, or store any cardholder data (CHD).

- No access to your Cardholder Data Environment (CDE).
- Atmoz's actions are confined to Azure control-plane data (metadata, billing, resource state).
- Solutions are architected to remain completely outside CDE boundaries.

Security & Compliance

Scope of Monitoring

- All data is non-sensitive, non-personal operational metadata: only operational resource and billing metadata is analyzed
- No scanning of customer app data or production content

Risk Management & Encryption

- All resource names are encrypted with tenant-specific keys both in transit and at rest, stored inside Azure's secure key vault
- Strict internal controls and least-privilege access employed

Incident Response

- Atmoz maintains a documented, regularly tested incident response plan aligned to ISO 27001 principles, covering detection, containment, analysis, mitigation, and notification

Malware and Threat Prevention

- Multi-layered malware controls: endpoint protection, vulnerability scanning, runtime behavioral detection
- Microsoft Defender for Cloud is deployed on all components
- Continuous monitoring and updating of controls

Segregation of Duties & Access Controls

- Strict role-based access within Atmoz (engineering, support, leadership)
- Ongoing compliance and threat monitoring
- Security controls include:
    - Encryption in transit and at rest.

- Multi-factor authentication (MFA).
- Network segregation and zero-trust principles.
- Continuous vulnerability management.
- Threat detection and compliance monitoring via Microsoft Defender for Cloud.

Governance & Control

Revocation & Data Lifecycle

- Customers can revoke Atmoz's access at any time (via Azure Lighthouse or the platform)
- All cached metadata is purged within 30 days or sooner upon request

Regulatory Compliance

Atmoz is aligned with Microsoft Cloud Security Benchmark controls for Azure workloads. Leveraging Microsoft Defender's solutions, Atmoz is compliant with the following regulatory compliance certifications:

- Microsoft Cloud Security Benchmark
- Azure CSPM
- ISO 27001:2013
- SOC 2

Customer Role in Maximizing Atmoz Value

To get the most out of Atmoz and to maintain a secure, effective, and compliant experience, customers play an active role in the following areas:

Granting and Managing Access

- Providing the required read-only Azure permissions (Global Reader, Monitoring Reader, Billing Reader) and User.Read.All permission.
- Scoping permissions to the appropriate subscription(s) or resource group(s).
- Revoking Atmoz's access when services are no longer required.

Maintaining Azure Environment Security

- Ensuring baseline Azure security controls (e.g., MFA, RBAC policies) are enforced for accounts used to grant Atmoz access.
- Maintaining compliance with their own internal and regulatory requirements.

Bot Installation and Configuration

- Installing the Atmoz Teams and/or Slack Bot in the relevant collaboration environments to enable proactive notifications.
- Configuring bot permissions and channels according to organizational policies.

Tagging and Metadata Accuracy

- Applying accurate resource tags and metadata to improve cost attribution and ownership identification.
- Keeping resource naming conventions up-to-date to avoid ambiguity.

Reviewing and Actioning Recommendations

- Evaluating Atmoz's optimization recommendations and taking appropriate action.

- Ensuring that approved changes are implemented in accordance with internal change management procedures.

Monitoring and Feedback

- Monitoring notifications and dashboards provided by Atmoz.
- Reporting any anomalies or suspected security incidents involving Atmoz's service to the Atmoz security team promptly.

Architecture & Workflow

Notification Workflow

- Atmoz requests Azure resource metadata every minute using your assigned permissions
- Data is encrypted in transit and at rest with unique keys per tenant
- When an issue is found, Atmoz only shares relevant case data directly to the appropriate user via your chosen collaboration platform (Teams, Slack or email)

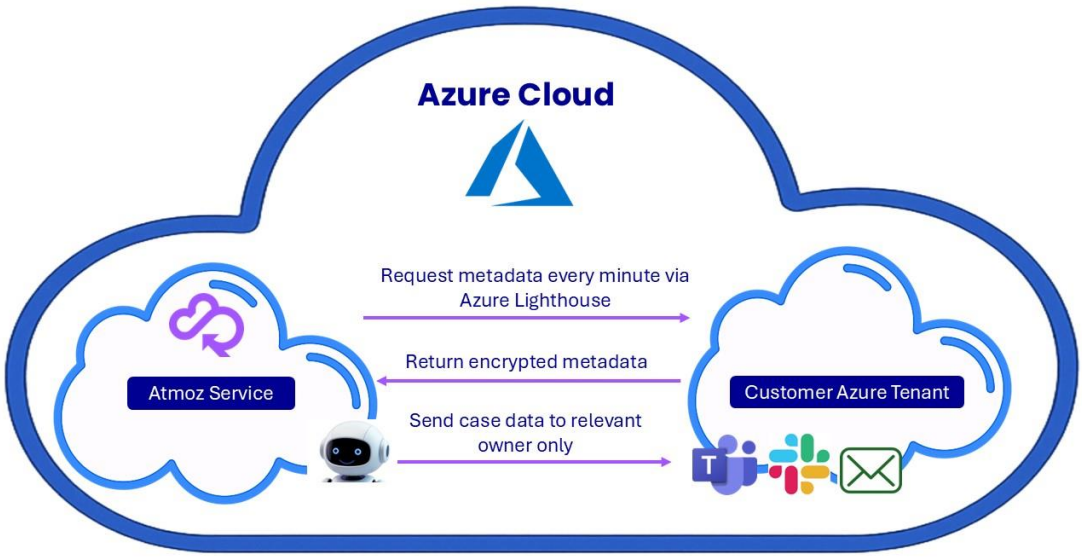
Sequence Diagram

The following sequence diagram illustrates how Atmoz interacts with your Azure environment and your communication channels:

1. Both Atmoz Service and Your Azure Tenant are Azure-Hosted:
   - Customer Azure Tenant (Azure): This represents your own Azure environment, where your resources and data reside.
   - Atmoz Service (Azure): This is the Atmoz monitoring and management service, which is also hosted within Azure for enhanced security and performance.
2. Data Collection Every Minute – Real Time:

- Request Metadata: Every minute, the Atmoz Service requests metadata about your Azure resources using the permissions granted via Azure Lighthouse.
- Return Metadata: Your Azure Tenant securely returns the requested metadata, which is encrypted in transit.
- Data Protection: Upon receipt, Atmoz encrypts any sensitive data such as resource names and user details before storing it, using a unique encryption key specific to your tenant.

3. Notification Delivery:
   - Send Notification: When an issue is detected or an action is required, Atmoz sends a notification to your Microsoft Teams or Slack bot. Only relevant case data is sent and only to the relevant owner.



Summary

Atmoz is designed from the ground up for security, compliance, and transparency:

- Only collects operational and cost metadata—never application data, secrets, or cardholder information.
- No “write” access or automated modifications to customer resources: humans always in control.
- Hosted on Microsoft Azure, leveraging market-leading security infrastructure and controls.
- No external data processors; customer data is never shared.
- Full control and immediate revocation of access by customers at any time.
- Maintains rigorous security governance, incident response, and malware prevention protocols.

For further information, technical documentation, or security certifications, please contact Atmoz’s security team at support@atmoz.co.

Atmoz is committed to making cloud cost optimization secure, transparent, and easy, for every organization.