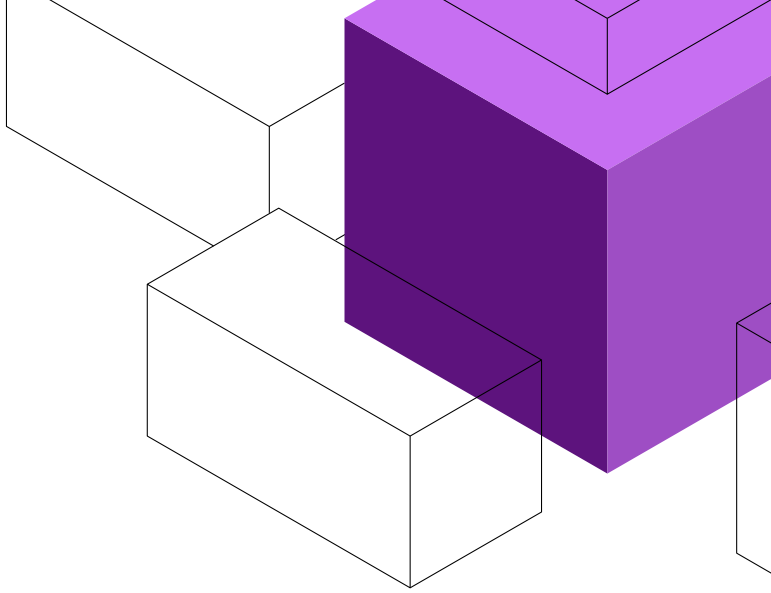
TiDB

DATASHEET

TiDB Cloud Shared Responsibility Model

Contents



Shared Responsibility

TiDB Cloud follows a shared responsibility model, in which PingCAP manages the platform infrastructure and its operations, while customers are responsible for configuring their accounts, applications, and data. The goal of this model is to clearly define each party's responsibilities and help ensure secure and compliant operations.

Responsibility Matrix

- **TiDB Cloud platform:** Refers to the PingCAP-managed TiDB Cloud service layer, including security and operations.
- **Cloud Customer (Fully-managed):** Refers to customers using TiDB Cloud's fully managed services (for example, Dedicated, Starter, or Essential), where the data plane is fully hosted and operated by PingCAP.

Responsibility Area	TiDB Cloud Platform	Cloud Customer (Fully-managed)
Cloud Infrastructure & Mgmt	• **Compute Management:** Manage EC2 instances, Kubernetes/EKS clusters. • **Storage Management:** Manage disk and S3 object storage, including data protection (e.g., backup) and support recovery from backup. • **Network Services:** Configure load balancers, DNS (Route 53), and provide PrivateLink endpoint service. • **Security Management:** Manage IAM, SSL/TLS certificates, and platform security. • **Monitoring & Compliance:** System monitoring, alerting, and TiDB Cloud security compliance.	No cloud infrastructure management required
Network & Connectivity	Provide Secure Connectivity (VPC Peering / PrivateLink / TLS) • **Private Connectivity:** Configure and maintain PrivateLink and VPC Peering between the TiDB Cloud control plane and data plane, including port-based access control for platform-to-cluster communication. • **TLS & Certificates:** Provision and manage certificates to enable encrypted cluster communication (issued via TiDB Cloud's certificate authority). • **Network Monitoring:** Continuously monitor and maintain network connectivity across key system components. • **Secure transmission of data:** Encryption and secure communication across all network traffic	Responsible for configuring application-side network access policies: • **Application Access Control:** Define and manage network access policies for applications connecting to TiDB Cloud. • **TLS Usage:** Require applications to establish secure connections to TiDB Cloud using TLS. • **Traffic Restrictions:** Enforce inbound and outbound traffic restrictions at the application layer as required.

Responsibility Area	TiDB Cloud Platform	Cloud Customer (Fully-managed)
Access Control & Auth	Responsible for delivering platform-level access control, identity integration, and security baseline capabilities: • **Identity & SSO Integration:** Support SSO (e.g., SAML, OIDC) and OAuth integration with third-party identity providers. • **Account Security Guidance:** Provide best practice guidelines for account and identity security configuration. • **Policy Enforcement:** Enforce web console account policies, including password complexity, rotation, and MFA requirements. • **Cluster Access Control:** Provide cluster account policies (including initial admin credentials) and enforce secure authentication. • **RBAC Capabilities:** Provide RBAC capabilities for both the TiDB Cloud web console and databases.	Responsible for database and application layer access control: • **Database User Management:** Create, manage, and secure database users and permissions. • **Database Role Management:** Assign and manage web console and database roles (RBAC). • **Credential Security:** Protect application secrets, keys, and passwords. • **Application Integration:** Configure applications to use secure authentication and follow platform policies. • **Usage of SSO Integration:** Configure and manage their identity provider for SSO/OAuth integration with the TiDB Cloud platform to ensure secure and compliant authentication. • **RBAC:** Manage TiDB Cloud web console RBAC and configure database RBAC.

Responsibility Area	TiDB Cloud Platform	Cloud Customer (Fully-managed)
Data Security & Encryption	Responsible for delivering encryption, secure transmission, and integration with industry-standard key management systems: • **Encryption at Rest:** Provide default encryption for data at rest (storage, backups, snapshots). • **Transmission encryption:** Provide TLS for the TiDB Cloud database cluster endpoint. • **Certificate Management:** Issue and manage certificates for cluster components to ensure trusted internal communication. • **KMS Integration:** Provide integration with cloud-native KMS for secure key storage and automated key rotation. • **CMEK Support (Optional):** Offer Customer-Managed Encryption Key (CMEK) capabilities, allowing customers to use their own encryption keys imported into their cloud KMS.	Responsible for protecting sensitive data within the database, managing encryption-related configuration, and ensuring secure access: • **Access Security:** Manage database users, enforce strong authentication, and configure encrypted connections. • **Certificate Usage:** Manage application-facing SSL/TLS certificates to ensure encrypted communication with the cluster. • **Data Operations:** Securely import, export, and back up data using encrypted channels. • **CMEK (Optional):** Enable CMEK in TiDB Cloud to encrypt data at rest using a symmetric encryption key that is under your complete control.

Responsibility Area	TiDB Cloud Platform	Cloud Customer (Fully-managed)
Audit, Monitoring & Alerting	Responsible for platform-level monitoring, logging, and auditing capabilities: • **System Monitoring:** Monitor platform and cluster health, performance, and resource utilization. • **Logging:** Collect system and application logs for operational visibility. • **Alerting:** Provide alerting mechanisms for critical platform events and anomalies. • **Audit Logging:** ◦ Maintain system-level audit logs to track platform changes, access events, and security-related actions. ◦ Deliver audit logs for identity and access activities to support security and compliance. • **Compliance Support:** Ensure logs and alerts meet security and compliance requirements.	Responsible for database-level monitoring, alerting, and compliance checks: • **Monitoring & Alerts:** Configure database and application-level monitoring and alert rules. Use the monitoring capabilities provided by the platform to oversee and manage cluster resource usage, ensuring resources are allocated appropriately. • **Log Review & Compliance:** Use platform-provided logs to perform security reviews, detect anomalies, and support compliance audits. • **Application Integration:** Ensure application-level logs and alerts are configured according to operational requirements.

Responsibility Area	TiDB Cloud Platform	Cloud Customer (Fully-managed)
Operations & Maintenance	Responsible for platform-level operations, maintenance, and availability: • **Version Management:** Deploy platform and cluster version upgrades. • **Patching & Updates:** Apply security patches and system updates to platform components. • **High Availability & Failover:** Ensure failover and service continuity in case of platform or cluster failures. • **Platform Backup & Recovery:** Maintain platform-level backup and recovery capabilities to protect customer data and platform state. • **Operational Monitoring:** Continuously monitor platform health and performance to prevent and respond to operational incidents.	Responsible for application-level maintenance and database schema management: • **Application Updates:** Manage and deploy upgrades to business applications. • **Operational Oversight:** Monitor application performance and maintain operational best practices.
	Responsible for platform-level support and issue resolution: • **Issue Diagnosis & Resolution:** Investigate and resolve platform, cluster, and system-level incidents. • **Remote Access (Authorized):** With customer approval, access the customer data plane via VPN or SSM for troubleshooting and case resolution. • **Audit Logging:** Maintain detailed audit records of all support activities, including remote access sessions, during the retention period.	Responsible for support and implementation of recommended changes: • **Business Context & Insights:** Provide relevant application and operational information to support personnel. • **Change Implementation:** Execute recommended database or application-level changes to resolve incidents.

Cloud Infrastructure & Management

The TiDB Cloud platform manages the underlying cloud infrastructure and management environment — including compute, storage, and control plane resources — so you don't have to.

Network & Connectivity

The TiDB Cloud platform provides secure and reliable connectivity options — including PrivateLink, VPC Peering, and TLS-encrypted connections — to keep your database traffic secure. You are responsible for managing application-side network access policies and ensuring secure connections to TiDB Cloud.

Access Control & Authentication

The TiDB Cloud platform supports multiple access control and authentication methods, including account permissions, role-based access, and multi-factor authentication. You manage database- and application-level users, roles, and access policies to ensure your business data remains secure.

Data Security & Encryption

The TiDB Cloud platform encrypts your data at rest and in transit by default, and supports integration with customer-managed key services (CMEK) if you need more control. You manage and protect your own keys, control who can access your data, and ensure that sensitive business data remains secure throughout its lifecycle.

Audit, Monitoring & Alerting

The TiDB Cloud platform collects and records system activity logs, and provides monitoring and alerting to help you quickly detect and respond to issues. You configure monitoring, alerting, and logging at the database and application levels to meet your operational and compliance requirements.

Operations & Maintenance

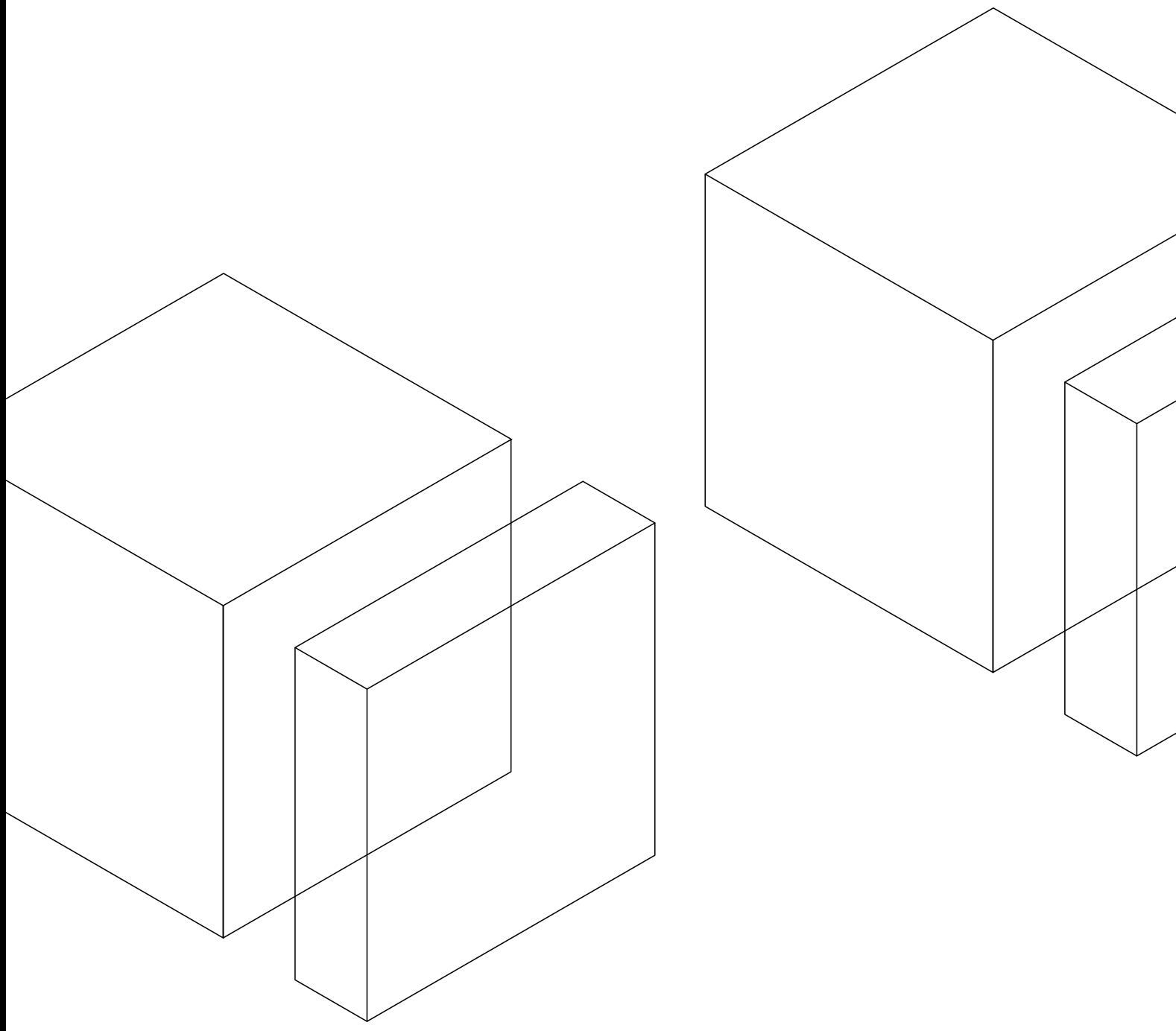
The TiDB Cloud platform handles system-level upgrades, patches, and high availability mechanisms so your service runs reliably. You take care of application-level operations, like schema changes, business-specific backup and recovery validation, and configuration management in your own application environment.

Support & Troubleshooting

PingCAP provides technical support and can assist with diagnostics when you authorize us to. You give us the necessary context and access when needed, and resolve issues related to your cloud environment and applications.

Compliance & Legal Notes

TiDB Cloud is designed and operated in alignment with industry-recognized security and compliance standards, including ISO, SOC, PCI-DSS, GDPR, and HIPAA. For more information on compliance practices and related legal guidance, please refer to the PingCAP Official Trust Center documentation.



EVALUATE TiDB FOR YOURSELF

Start Your Free Trial

Contact us for a personalized demo at pingcap.com/demo/