



WHITE PAPER

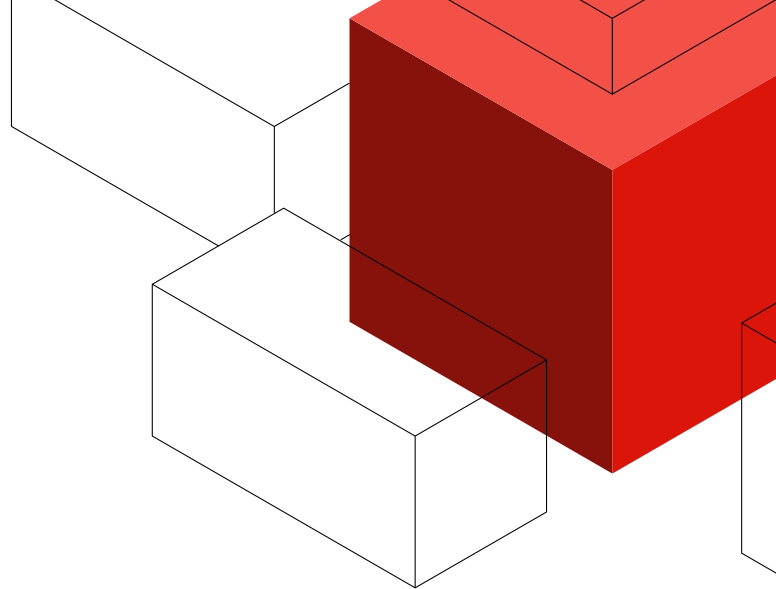
TiDB Cloud Security

Version 1.0



Contents

Introduction	3
Platform Security Architecture	4
Data Protection	11
Access Control	13
Observability and Incident Response	17
Compliance	19
BYOC Model Considerations	22
Defect Management Process	24
Infrastructure Operations	27



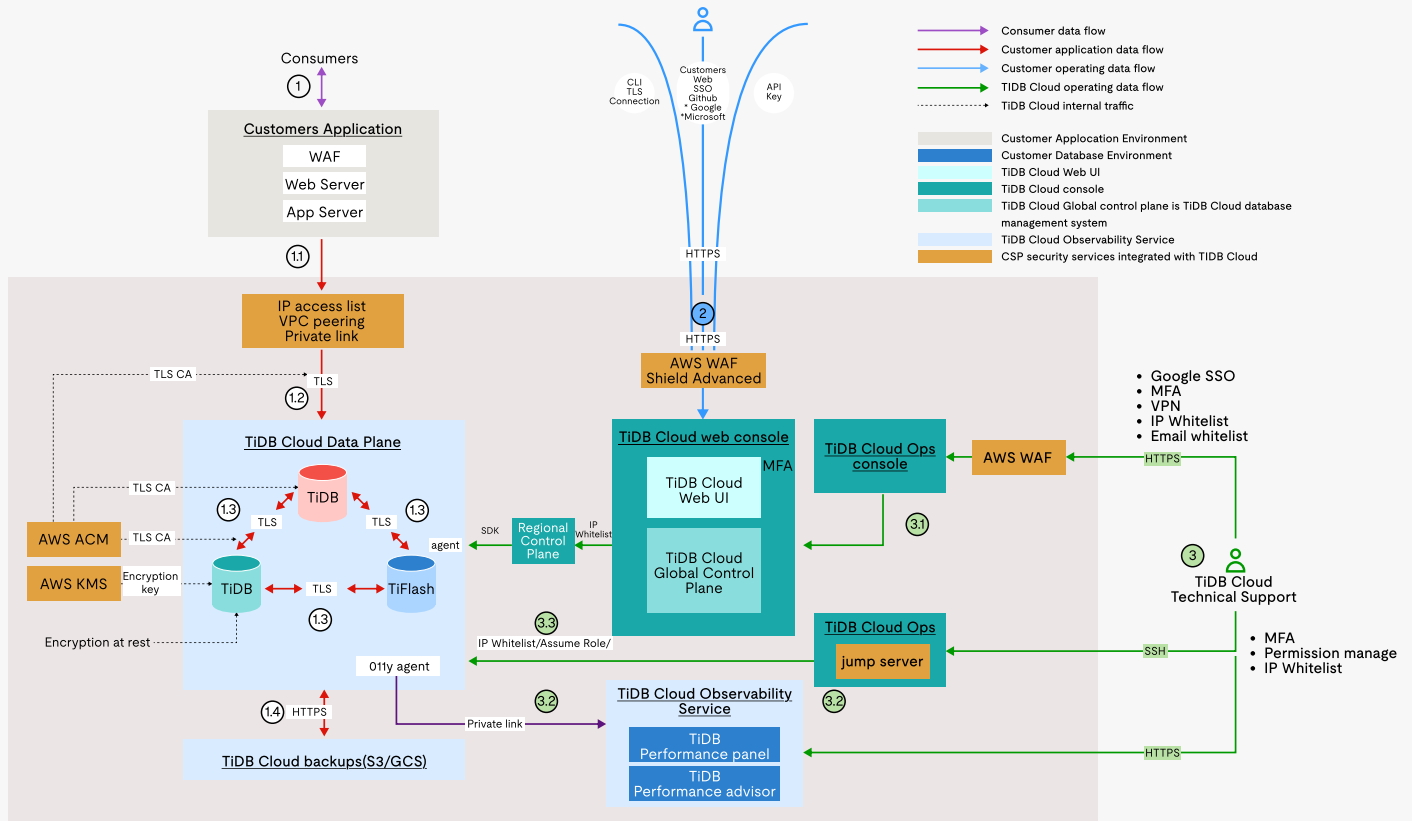
Introduction

PingCAP is committed to building trust in TiDB Cloud through a rigorous adherence to Trust principles, ensuring that security is not an afterthought but a foundational pillar of our cloud database platform. At the core of this commitment is a secure-by-design architecture, engineered to eliminate unnecessary trust assumptions and enforce granular controls across every layer of the system. From the multi-region, per-tenant isolation of our Kernel/NextGen architecture to the strict separation of control plane and data plane responsibilities, TiDB Cloud is purpose-built to minimize attack surfaces and protect customer data at every stage of its lifecycle.

In an era where data security defines enterprise trust, TiDB Cloud sets a new benchmark for DBaaS excellence. By prioritizing secure-by-design features, we meet and exceed global industry security standards. Whether deploying in shared, dedicated, or BYOC environments, TiDB Cloud delivers the confidence enterprises worldwide need to innovate without compromising on protection.

Platform Security Architecture

TiDB Cloud's architecture is built on a security framework that puts emphasis on explicit component isolation, role-based workflows, and multi-layered trust boundaries. Below is a structured overview focusing on security and trust mechanisms.





NO.	Data Flow Description	Optional Security Technology Controls
1	Data flow between customer's application and	customer's TiDB clusters on TiDB Cloud
1.1	Consumer sensitive data is collected and owned by TiDB Cloud customers.	TiDB Cloud has no visibility and control permission for consumer sensitive data. Customers can deploy security protection and encryption measures for applications.
1.2	Customers transmit consumer sensitive data and business data via their application to TiDB database cluster.	IP access list should be set up to allow trusted app IP to access your TiDB database cluster. Private Link should be enabled to secure the data transfer connection (only available on AWS and for Dedicated Tier). VPC Peering privatizes customers' VPC routing traffic and isolates it from the public internet network (only for Dedicated Tier).
1.3	Customers transmit their data between different TiDB components in the same cluster.	Mutual TLS is used in communications between different TiDB components in the same cluster. A distinct set of certs are issued for each cluster.
1.4	Customers may use AWS S3 bucket for data storage, as well as data backup and snapshot.	All data stored in TiDB is encrypted via TiDB Cloud managed keys. All backup files are stored in per-cluster S3 / GCS buckets with default encryption. Default keys are managed on AWS KMS. Additionally, TiDB Cloud supports the CMKE feature, allowing customers to import their own keys stored in AWS KMS to encrypt TiDB Cloud's S3/EBS.



NO.	Data Flow Description	Optional Security Technology Controls
2	Data flow between customer technicians and customer's TiDB Cloud Web Console	
2.1	Customers access and operate their own TiDB database clusters via open API, Cli and SSO users,such as Google workspace, Github.	TiDB Cloud is equipped with WAF to monitor malicious web traffic from the Internet. TiDB Cloud supports HTTPS protocol by default to protect the data transmission security between client browsers and TiDB Cloud console. TLS is by default for connecting to customer TiDB cluster, Customers can configure client (MySQL / MyCli) and TiDB Cloud.
3	Data flow between PingCAP technical support and TiDB Cloud Service Central	
3.1	The creation and configuration of customer TiDB database clusters are centrally managed by TiDB Cloud Service Central. Only technical personnel designated by PingCAP can access and maintain TiDB Cloud Service Central through TiDB Cloud OPS.	The access of technicians designated by PingCAP must meet the following conditions: 1. TiDB Cloud OPS may be accessed only via VPN; 2. TiDB Cloud OPS may be accessed only by approved technicians on the IP white list and Email white list; 3. TiDB Cloud OPS may be accessed only via Single Sign-On (SSO) and Multi-Factor Authentication (MFA); 4. All traffic accessing TiDB Cloud OPS will be inspected by WAF. 5. RBAC is combined with time-based access management policies to ensure controlled and timely access. 6. All traffic and operational accessing TiDB Cloud OPS will all be audited. 7. The technicians designated by PingCAP will participate in security training every year and need to pass the SOC2 security test.



NO.	Data Flow Description	Optional Security Technology Controls
3.2	TiDB Performance panel: Allows visibility to metadata, including queries that may contain consumer data in customer queries – data in transit only. TiDB Performance advisor: Slow query log lines directed to the TiDB Cloud backend for analysis and index suggestions. The system metadata may include audit logs that capture SQL statements executed against customer databases, potentially involving consumer-sensitive data. To uphold privacy and compliance, TiDB Cloud applies robust log redaction and masking techniques—ensuring that personally identifiable information (PII), protected health information (PHI), and PCI-sensitive data are either redacted or omitted entirely.	1. TiDB Cloud support personnel use SSO to access the observability service for diagnosing cluster status. 2. Within the observability service, any content involving user-sensitive information is masked to prevent exposure, and access is strictly governed by RBAC-based controls. 3. The observability agent operates within the data plane, establishing communication with the server side via IP allowlists and assume-role authentication.
3.3	This link pertains to situations where, in the event of a failure in the customer’s cluster infrastructure, PingCAP support personnel need to log into the customer dataplane and TiDB Cloud to perform operational maintenance tasks. All processes are handled through Bastion for login procedures and logging of the handling information.	1. All logins must be conducted through Bastion for operations and maintenance. 2. Access to Bastion itself is restricted to the office intranet, and MFA is enabled on the login side. 3. Access to user and management interface infrastructure is via Bastion, and all command-line operations are audited by Bastion. 4. The security team analyzes the audit log contents every two weeks to identify obvious commands and abnormal behaviors.



1. Core Components: GCP, RCP, and Data Plane Separation

The architecture is segmented into three critical planes to enforce functional and security isolation:

- **Global Control Plane (GCP):** Manages cross – region and multi – tenant configurations, including identity, policy enforcement (e.g., encryption keys), global monitoring, billing, account management, and API gateway operations. It centralizes governance for features like encryption keys, compliance settings, and cross – region consistency.
- **Regional Control Plane (RCP):** Handles region-specific operations, such as cluster provisioning, cloud resources, network configuration (e.g., VPC peering, PrivateLink), and local monitoring. It bridges GCP policies with regional execution.
- **Data Plane:** Hosts customer data and application workloads (e.g., TiDB, TiKV, TiFlash nodes). Access is strictly controlled via customer-managed credentials or authorized support workflows.

2. Trust Boundary Isolation

Trust boundaries are enforced across three dimensions to prevent unauthorized cross-tenant or cross-region access:

- **Multi-region Isolation:** RCPs in distinct regions operate independently. Data residency is enforced via regional storage, and cross – region replication (if enabled) uses encrypted, private links. The independent operation of RCPs ensures that any security incident in one region does not affect others.
- **Per-tenant Isolation:** Each tenant's resources (clusters, network configurations, and logs) are isolated at the GCP and RCP levels, leveraging unique identifiers (e.g., Tenant IDs) and role – based access controls (RBAC). This isolation ensures that one tenant's data and operations are not accessible to others.
- **Cross-account Isolation:** In Bring-Your-Own-Cloud (BYOC) deployments, customer AWS/GCP accounts are isolated from PingCAP – managed accounts via PrivateLink, ensuring no shared infrastructure. The data plane under the customer's account VPC further enhances this isolation.



3. Role and Workflow Based Separation

Workflows are segregated by role to enhance transparency, critical for enterprise compliance:

- **Support Operations:** Access to customer environments is restricted to authorized personnel via bastion hosts and manual approval workflows. Audit logs track all interactions, including control plane changes.
- **Customer Operations:** Customers manage clusters via the TiDB Cloud Console or APIs, with permissions governed by RBAC (e.g., Project Owner, Billing Admin). Data plane access (e.g., SQL queries) is customer-exclusive unless explicitly authorized.
- **Cluster Data Flow:** Data movement (e.g., between TiDB, TiKV, and external applications) is encrypted end-to-end (TLS 1.3 in transit, AES-256 at rest) and isolated from control plane traffic. Customer data never mixes with operational logs.

4. Tenant Isolation

Tenant isolation varies by deployment model to meet diverse enterprise needs:

- **Dedicated:** Single-tenant clusters with exclusive access to underlying infrastructure (compute, storage). Control plane operations managed by PingCAP with customer visibility.
- **Starter and Essential:** enforces isolation by routing requests through a tenant-aware gateway, allocating compute resources per tenant for independent workloads, and partitioning data into Raft-replicated tenant private regions — ensuring robust isolation across network, compute, and storage layers.
- **BYOC:** Clusters deployed in customer-managed AWS/GCP accounts, with network isolation. Control plane (e.g., monitoring) may be hosted by PingCAP or the customer, requiring explicit authorization for data access.

5. Network Isolation Models

TiDB Cloud supports three network isolation mechanisms to secure data in transit:

- **VPC Peering:** Provides direct private connection between customer VPCs and TiDB Cloud VPCs (non-overlapping CIDRs), available for Dedicated and BYOC tiers.
- **PrivateLink:** Creates a private endpoint for secure, one-way communication between customer applications and TiDB clusters, eliminating public internet exposure (preferred for high-security environments).
- **IP Whitelist:** Restricts cluster access to predefined IPv4 CIDRs
- **Security Groups & NACLs:** TiDB Cloud adopts a default-deny posture at the network layer. Security groups only open the minimum required ports, scoped to specific source IPs, and network ACLs provide coarse-grained subnet-level controls. This ensures traffic between control plane, data plane, and customer applications is tightly restricted and continuously aligned with least-privilege principles.
- **PrivateLink for Control Plane; No Public Internet Exposure:** PrivateLink secures control plane access, preventing public internet exposure. It offers CIDR-free planning and enhanced security, with traffic isolated between the customer's VPC and TiDB Cloud. Currently supported only in AWS

6. Security Responsibilities by Tier

Tier	Security Focus	Key Features
Global Control Plane (GCP)	Global governance and compliance	Identity and policy management, KMS integration for encryption keys, global audit log aggregation, cross-region policy enforcement
Regional Control Plane (RCP)	Regional isolation and operations	VPC peering and PrivateLink configuration, regional IAM scoping, regional monitoring/alerting pipelines, localized compliance enforcement
Data Plane	Customer workload protection	mTLS between cluster components, TLS 1.3 ingress for applications, AES-256 encryption at rest (TiKV/TiFlash/EBS/S3), CMEK/BYOK for Dedicated/BYOC



7. Stateless vs. Stateful Components

Components are classified to optimize resilience and security:

- **Stateless Components:** API gateways, load balancers, and monitoring services. Easily replicated across regions to reduce single points of failure.
- **Stateful Components:** TiDB, TiKV, and TiFlash nodes (store customer data). Designed with high availability (multi-AZ deployment) and strict access controls to prevent data corruption.

This architecture ensures TiDB Cloud aligns with industry standards (defense-in-depth) while addressing enterprise concerns like data residency, operational transparency, and compliance.

Data Protection

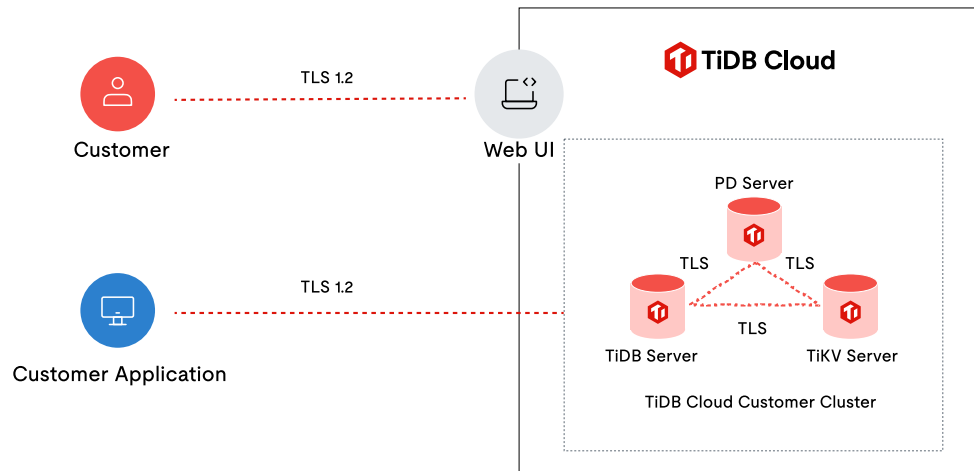
Data Protection Mechanisms in TiDB Cloud

1. Encryption at Rest

- **S3-based SSE (per-tenant buckets, default SSE):** TiDB Cloud uses S3-managed SSE-S3 encryption for S3-related clusters. Snapshot and database backup files are automatically encrypted and stored in per-tenant S3/GCS buckets with default encryption enabled (keys managed by AWS/GCP).
- **EBS Backup Encryption (per-tenant):** EBS volumes for TiDB clusters (e.g., TiKV and TiFlash) are encrypted using AWS KMS/EBS keys, ensuring per-tenant encryption of storage media.
- **Local Encryption (TiKV/TiFlash AES-256):** Data stored in TiKV and TiFlash is encrypted locally using AES-256 encryption, a standard for securing data at rest.
- **CMEK for BYOC and Dedicated:** Customer-Managed Encryption Keys (CMEK) enable customers to use their own cryptographic keys to encrypt static data in both Bring-Your-Own-Cloud (BYOC) and Dedicated clusters. Once enabled, all cluster data and backups within the tenant use the CMEK .

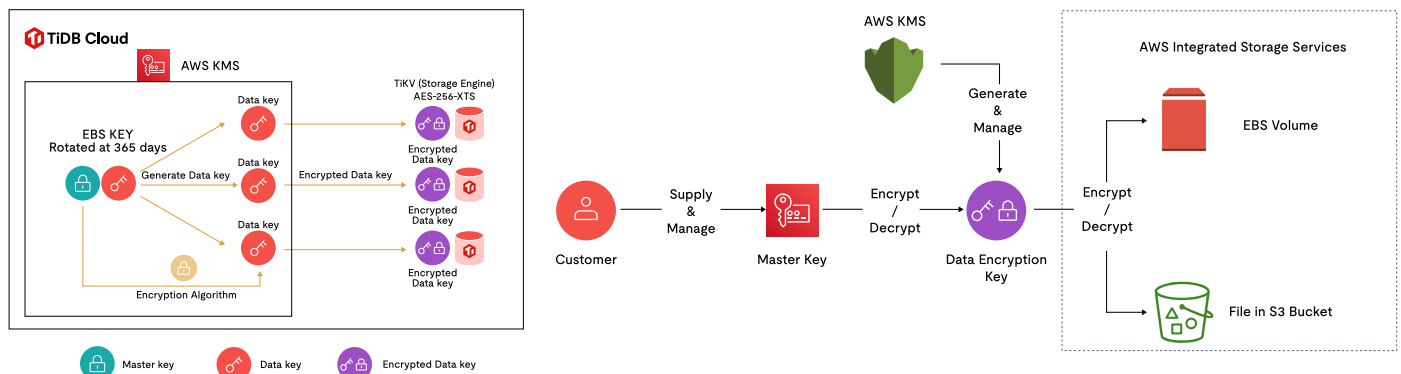
2. Encryption in Transit

- **mTLS Between Internal Components (per-cluster certs, CA download for verification):** Mutual TLS (mTLS) is used for communications between TiDB components (TiDB, PD, TiKV) within the same cluster, with certificates issued per cluster. Customers using Dedicated Tier can download CA certificates from the console for client-side verification.
- **TLS for Customer Ingress:** TLS 1.3 is supported for customer ingress connections. While TLS 1.2 is enabled by default for compatibility, TLS 1.3 can be manually configured. Server-side enforcement is possible via SET `GLOBAL require_secure_transport=ON`.



3. Key Management

- **AWS/GCP KMS Usage:** Data and encryption keys are managed via AWS/GCP KMS. Data encryption keys (DEKs) are encrypted using master keys (CMKs) and stored with data, ensuring no unencrypted keys are persisted.



- **DEK/CMK Hierarchy:** Keys follow a DEK (Data Encryption Key)/CMK (Customer Master Key) hierarchy, where CMKs encrypt DEKs, and DEKs encrypt data.
- **BYOK Support for Enterprise Customers:** Bring-Your-Own-Key (BYOK) is supported for enterprise customers, allowing them to use their own keys for enhanced control over encryption.



4. Baseline Hardening Practices

TiDB Cloud enforces hardened baselines across Kubernetes, AWS, and storage infrastructure to minimize attack surface and maintain compliance:

- **EKS/Kubernetes** – API server endpoints are restricted to private access; IAM Roles for ServiceAccounts and Security Groups for Pods enforce least-privilege; Pod Security Standards and NetworkPolicies deny all traffic by default unless explicitly required.
- **AWS S3** – All buckets block public access, enforce default encryption, TLS in transit, and enable versioning and Object Lock for critical backups.
- **Servers & OS Images** – All servers use official, minimal images with passwordless login disabled; direct root login is prohibited. Patch management is automated through AWS Systems Manager.
- **Audit & Logging** – EKS control plane logs (API, Audit, Authenticator, Scheduler) are enabled and streamed to CloudWatch for centralized monitoring.

Access Control

TiDB Cloud delivers a robust identity, access control, and authentication (IAA) framework designed to balance security, flexibility, and compliance. Below is a structured breakdown of its key components, aligned with modern cloud database standards.

1. User & API Key Authentication (JWT, OAuth 2.0)

TiDB Cloud supports multiple authentication methods to secure user and programmatic access:

User Authentication:

- **Password & SSO:** Users can log in via email/password (credentials stored in Auth0 using industry-standard one-way hashing) or SSO (Google Workspace, GitHub, Microsoft, or enterprise OIDC/SAML). SSO users rely on their identity provider (IdP) for MFA.
- **JWT:** Used for user identity verification (e.g., internal operations and cross-account access). JWT tokens are validated via public keys from AWS KMS, ensuring secure mapping to database accounts .



API Key Authentication:

- Administrators can create organization-scoped API keys for programmatic access. Key usage requires enabling an organization-level API access list, and all key creation/deletion events are logged in the console audit.

OAuth 2.0:

- Supports two grant types:
 - **Authorization Code:** For web apps, requiring user authorization to generate tokens.
 - **Device Code:** For limited-input devices (e.g., IoT), where users confirm a code via a browser to grant access.
- Tokens (access/refresh) are used to call TiDB Cloud APIs, with refresh tokens enabling secure token renewal.

2. Console & API Role Enforcement

TiDB Cloud enforces granular permissions through role-based access at both console and API levels:

Console Roles:

- **Organization-Level Roles:** Four predefined roles (Owner, Billing Admin, Console Audit Admin, Member) with distinct permissions:
 - **Owner:** Manages projects, invites users, and controls organization settings.
 - **Billing Admin:** Views/edits payment information.
 - **Console Audit Admin:** Manages console audit logs.
 - **Member:** Views organization and project details.
- **Project-Level Roles:** In development, with plans to extend role-based control to projects (targeting fine-grained access by 2025) .

API Role Enforcement:

- API access is governed by the same organization/project roles. For example, only Owners or Billing Admins can modify payment settings via API .



3. RBAC: Current State & Fine-Grained Roadmap

TiDB Cloud's RBAC system evolves to meet growing demands for precision:

Current RBAC:

- **Three-Tier Hierarchy:** Organizations → Projects → Clusters, with permissions managed at the organization level. Roles include static privileges (e.g., table access) and dynamic privileges (e.g., database management).
- **MySQL Compatibility:** Roles and accounts are stored in the `mysql.usersystem` table, supporting nested roles but no built-in roles.

Fine-Grained Roadmap (2025+):

- **Two-Tier Resource Hierarchy:** A new structure (Organizations → TiDB instances) with optional TiDB groups, simplifying IAM and enabling cluster-level role assignment.
- **Independent RBAC Tables:** Introduces dedicated `rbac_role_bindings` for authorization checks, decoupling RBAC logic from business resource associations.

4. Bastion/Break-Glass Access Limitations

TiDB Cloud restricts emergency access to minimize unauthorized intervention:

Manual Operations Policy:

- PingCAP support teams access customer clusters via bastion hosts only after user authorization and security team approval.
- Access requires:
 - SSO/MFA authentication.
 - AWS IAM permissions (least-privilege model).
 - IP whitelisting and VPN usage.
- All activities are logged in bastion and reviewed weekly.
- **Break-Glass Scenarios:** Temporary access is time-bound and revoked immediately post-resolution. Audit logs track all break-glass events for compliance.

5. Access to Customer Environments: Who, When, How

Access to customer data is strictly controlled based on user type and context:

User Type	Access Method	Controls
Customer Employees	Console (SSO/password) or SQL client	RBAC roles, IP whitelisting, VPC peering, or Private Link.
Customer Apps	OpenAPI (API Key) or TiDB Cluster (API KEY)	IP whitelisting, TLS encryption, and API access lists.
PingCAP Support	Observability Service or Bastion (emergency)	SSO/MFA, least-privilege IAM roles, IP whitelisting, and real-time audit.

6. Audit Logging for Control Plane & Data Access

TiDB Cloud logs all critical events to enable traceability and compliance:

- **Control Plane (Console Audit):** Records user actions (e.g., account registration, login) with timestamps, user IDs, and event outcomes.
- **Data Plane (Database Audit):** Logs SQL operations (e.g., CONNECT, DDL, DML) on clusters, including user, SQL statement, and execution result. Disabled by default.

7. MFA/SSO Split: Policy & Implementation

TiDB Cloud differentiates MFA requirements based on SSO usage:

- **SSO Users:** MFA is enforced at the IdP level (e.g., Google Workspace, GitHub). TiDB Cloud does not configure MFA for these accounts.
- **Non-SSO Users:** MFA (e.g., Google Authenticator) is optional for users managed via Auth0, enhancing security for password-based logins.

This framework ensures TiDB Cloud balances security with usability, adapting to evolving enterprise needs while maintaining compliance with global standards.

Observability and Incident Response

PingCAP maintains a comprehensive observability and incident management program for TiDB Cloud, designed to ensure service availability, performance, and rapid mitigation of issues affecting customer workloads. These capabilities operate within TiDB Cloud's shared responsibility model, where PingCAP is responsible for the security, monitoring, and resilience of the managed service infrastructure, while customers manage the configuration and security of their own applications and data.

1. Observability and Monitoring

TiDB Cloud provides an integrated observability suite that offers real-time visibility into system health, query performance, and operational history:

- **Metrics and Dashboards** – Real-time visualization of CPU, memory, disk I/O, latency, QPS, and TPS across clusters, using dedicated performance dashboards.
- **Logs** – Automatic collection of runtime logs from core components (TiDB, TiKV, PD) for troubleshooting and root cause analysis.
- **Alerts** – Built-in alerting rules to detect abnormal states, excessive resource usage, or component failures, notifications are delivered via email, Webhook, or SMS.
- **SQL Performance Analysis:**
 - **Slow Query Logging** – Captures execution details for queries exceeding configured thresholds, with plan comparison and execution time distribution.
 - **TopSQL** – Identifies high-resource-consuming queries in real time.
 - **Key Visualizer** – Heatmap visualization of key distributions to detect hotspots.
 - **Profiles** – Continuous performance profiling for rapid diagnosis.
- **Event Tracking** – Historical record of cluster-level changes, incidents, and operational events.

Additional security-related monitoring includes:

- **Security Log Monitoring** – AWS CloudTrail and TiDB audit logs track administrative actions and database events.
- **Vulnerability Scanning** – Amazon Inspector and Snyk scan for host and code vulnerabilities.
- **Network Traffic Monitoring** – VPC Traffic Mirroring and AWS CloudWatch analyze network traffic for anomalies.
- **Threat Detection** – Amazon GuardDuty detects malicious activity, unauthorized access, and potential data exfiltration.



2. Incident Detection and Response

PingCAP maintains a structured incident management process aligned with industry best practices:

- **Detection and Alerting** – Automated alerts trigger based on system metrics, security events, or anomalous behavior.
- **Triage and Investigation** – Security and OPS teams assess impact, determine root cause, and prioritize incidents based on severity and customer impact.
- **Secure Troubleshooting Access** – Engineer access to customer clusters is via bastion hosts, with enforced SSO, MFA, and full audit logging.
- **Post-Incident Review** – Following resolution, a post-mortem is conducted to document root cause, corrective actions, and long-term prevention measures.

3. Customer Communication and Transparency

- **Customer Notification** – In the event of a confirmed security incident affecting customer data or service availability, PingCAP will notify affected customers without undue delay, following applicable regulations.
- **Status Updates** – Customers receive ongoing updates during active incidents via agreed communication channels.
- **Post-Incident Reports** – Summary reports are provided upon request, outlining incident details, impact, remediation steps, and prevention measures.



Compliance

TiDB Cloud's compliance program and customer self-service controls are purpose-built to support highly regulated industries while fostering operational transparency. At PingCAP, we adhere to industry-leading standards and provide strong governance around audit readiness, data residency, and customer control—aligned with frameworks such as SOC 2, ISO 27001/27701, HIPAA, GDPR, CCPA, and PCI-DSS. Through our “Trust Hub,” we openly communicate compliance commitments and certify third-party validations.

Compliance Certifications

SOC 2 Type II

- TiDB Cloud undergoes recurring SOC 2 Type II examinations, validating our controls across security, availability, and confidentiality over a sustained period. Independent audit reports are made available to customers under NDA.

ISO/IEC 27001:2013 & ISO/IEC 27701

- Certified by BSI in July 2021, our ISMS covers the full lifecycle of service development and operations. We extend this framework through ISO 27701 privacy extension to address GDPR and CCPA privacy requirements, with active surveillance audits to ensure continuous compliance.

GDPR, CCPA, HIPAA, PCI-DSS, EU-US Data Privacy Framework

- TiDB Cloud aligns with widely adopted regulatory regimes for personal data protection and privacy. We've implemented governance protocols to help customers meet GDPR, CCPA, HIPAA, and PCI-DSS obligations and support safe data transfers under the EU-US DPF.

SOC 1 and SOC 3 Public Reporting

- In addition to SOC 2, we support SOC 1 and SOC 3 frameworks, with SOC 3 reports publicly available to offer transparency into our overall compliance posture.



Data Residency & Sovereignty

Region-Based Deployments

- Customers can select specific AWS or GCP regions when deploying TiDB Cloud clusters—ensuring that data (primary and backups) stays within defined geographic boundaries unless explicitly configured otherwise.

Optional Multi-Region Backups

- For high availability and disaster recovery requirements, Dedicated Tier supports dual-region backup replication under customer control. Cross-region replication is disabled by default and requires explicit configuration.

Encryption & Key Management

- Data at rest is encrypted by default using provider-managed keys. For customers requiring stronger control, Customer-Managed Encryption Keys (CMEK) are supported by Dedicated Tier, enabling full key ownership via AWS KMS.

Customer Self-Service Controls

Secure Data Deletion & Project Termination

- Customers have console-level capabilities to delete clusters and terminate projects. Deletion is managed in alignment with NIST SP 800-88 standard for secure media sanitization. Actions are tracked via audit logs.

Dedicated Tier Network Access Controls

- IP Whitelist: Configure inbound IP/CIDR allowances (up to 100 entries per cluster) via UI, modifications are logged and restricted to project-level owners.
- Private Connectivity: Supports AWS PrivateLink, GCP Private Service Connect, and VPC Peering to isolate DB traffic from the public internet.

Export & Integration Controls

- Customers can export logs, metrics, and backups to their designated storage endpoints under controlled conditions. Export access follows least-privilege IAM policies and write-only permissions. Integration with external monitoring systems like Datadog is fully supported.



Security Governance & Auditing

Authenticated Access & MFA

- Console/API access requires authenticated sessions via SSO (OIDC/SAML) or verified platform accounts. MFA is enforced for non-SSO users.

Audit-Ready Controls

- All changes to compliance-sensitive settings (e.g., IP lists, export policies) are subject to authenticated operations and are logged for full traceability and audit purposes.
- Completeness: The audit system captures every occurrence of each supported event types. Log entries are typically available for viewing, download, and programmatic access via the API within 60 minutes of the event occurrence.
- Append-only storage: Once an event is recorded, its content cannot be modified or deleted. The audit log operates as an append-only data store.
- No manual deletion allowed: You cannot manually delete audit log entries. Logs are automatically cleaned up based on the 90-day retention policy.
- Audit of audit management: Operations that change the audit logging configuration (such as Enable-ConsoleAuditLog) are themselves recorded as audit events, providing a tamper-evident trail of audit log administration.

In-Flight & Intra-Service Encryption

- Transport Layer Security (TLS 1.2/1.3) is enforced for client access, internal service components (TiDB, TiKV, PD) also leverage mTLS for secure service-to-service communications.



BYOC Model Considerations

1. Network Isolation

In BYOC deployments, TiDB Cloud ensures robust isolation between PingCAP services and customer environments. Connectivity is established using private channels such as AWS PrivateLink.

- PrivateLink (AWS only) exposes a private endpoint for one-way access to TiDB Cloud resources, further minimizing external exposure. This model ensures all customer traffic remains on secure private networks.

2. Identity and Access Management

- In BYOC mode, the customer's dataplane services are deployed within the customer's own cloud account. Cross-account permission delegation is used to authorize PingCAP to perform service initialization and system upgrades. PingCAP ensures that the delegated policies adhere to the principle of least privilege, and the customer retains full control over permission granting.
- Operational access for PingCAP engineers is controlled via bastion hosts, MFA, and just-in-time approval workflows.
- All actions are recorded in detailed audit logs, providing transparency and accountability.

3. Encryption and Key Management

BYOC deployments integrate with customer-managed KMS for encryption at rest.

- Customer Master Keys (CMKs) remain under customer control; PingCAP systems never have direct access to raw key material.
- Keys are only used for encrypt/decrypt operations within the customer's cloud account, with code reviews enforcing correct usage.
- This model ensures customers maintain ownership of their encryption lifecycle and compliance posture.



4. Threat Modeling and Compensating Controls

Because BYOC introduces unique risks—such as misconfigured customer accounts, data leakage in transit, or IAM over-permissioning—PingCAP incorporates additional safeguards.

- Regular architecture reviews and penetration testing validate controls.
- Threat modeling identifies attack paths specific to shared-responsibility deployments.
- Compensating measures include enforced network isolation, scoped access, and continuous monitoring.

5. Audit Logging and Observability

Audit and monitoring responsibilities are explicitly divided between PingCAP and the customer.

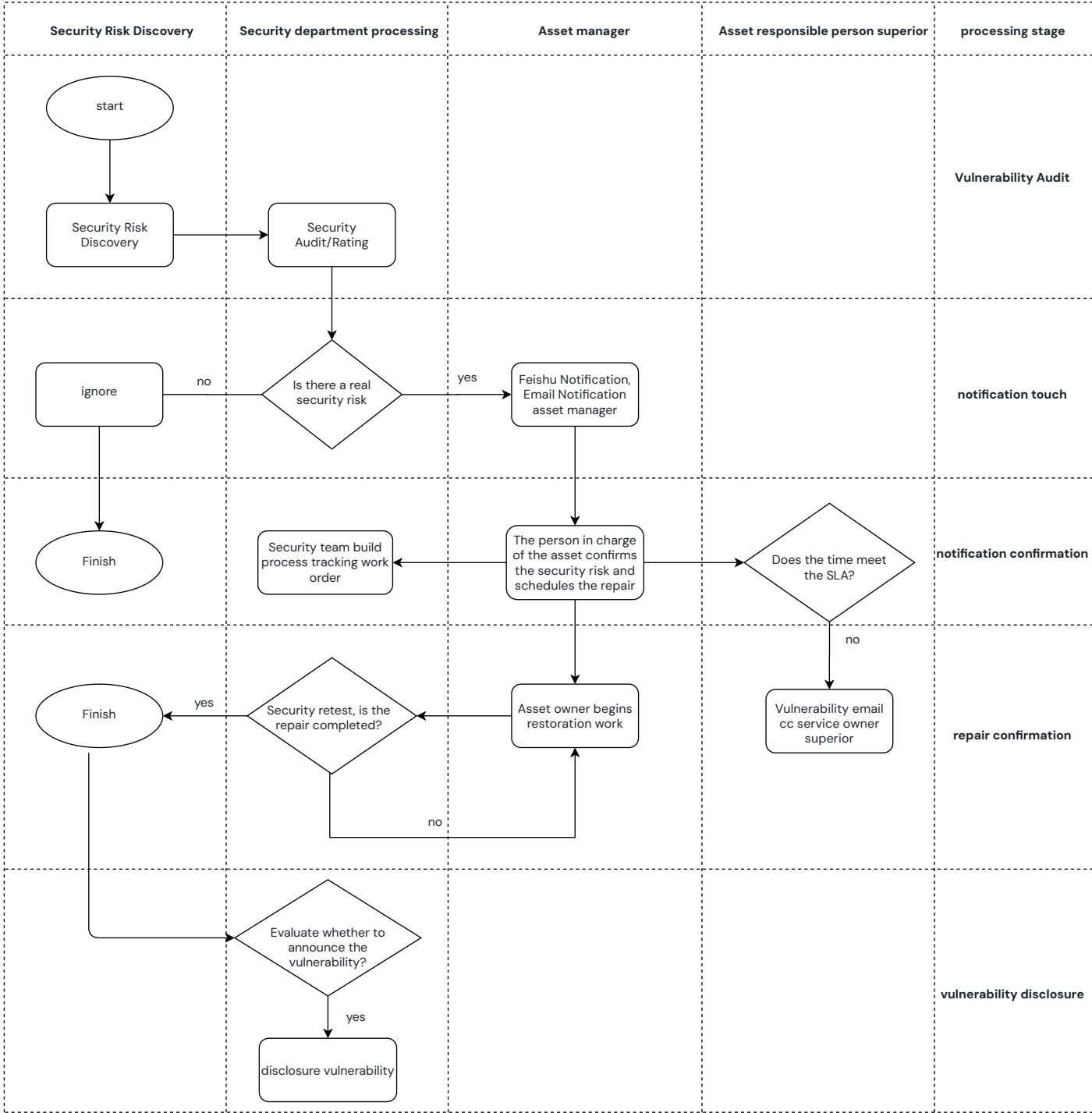
- TiDB Cloud logs all operational activities, including access events, configuration changes, and troubleshooting steps.
- Customers can export logs to their own SIEM platforms for correlation and incident response.
- Metrics and alerting flow from the data plane to regional/global control planes, ensuring centralized monitoring with customer visibility.



Defect Management Process

We have established a systematic defect management process that covers the entire product development and operations lifecycle, ensuring that defects are promptly identified, quickly remediated, and effectively prevented from recurring.

- **Centralized Risk Management:** All defects are tracked in a unified defect management platform. A security ticket is not formally closed until security engineers have completed retesting and verified that the issue has been properly resolved.
- **Priority Assessment:** We use the international CVSS 3.1 scoring standard together with business impact analysis to classify and prioritize vulnerabilities, ensuring that critical risks are addressed first.
- **External Validation:** At least once a year, we engage independent third-party security firms to perform penetration testing, identifying potential risks from an external perspective.
- **Internal Validation:** During defect handling, our internal security team proactively detects and mitigates potential issues using static code analysis, security design reviews, image scanning, and internal penetration testing.
- **Threat Intelligence Monitoring:** Our security team tracks industry intelligence and CVE disclosures to stay aware of risks and respond quickly.



Customer Notification

- For critical security incidents, we proactively notify customers through official announcements or email communications. This ensures that customers are promptly informed of potential risks and can take appropriate actions to protect their environments.
- For self-managed deployments, detailed information on component-related CVEs is publicly disclosed on our official security page. Customers can access the latest security advisories, patch information, and mitigation guidance at any time: <https://www.pingcap.com/security/>.
- Our goal is to maintain transparency and keep customers informed, enabling them to confidently manage and secure their database deployments.



Infrastructure Operations

We have established a systematic defect management process that covers the entire product development and operations lifecycle, ensuring that defects are promptly identified, quickly remediated, and effectively prevented from recurring.

Backup & recovery reliability

TiDB Cloud provides built-in backup and recovery reliability through automatic snapshot backups applied by default across all cluster tiers, as well as optional manual backups for Dedicated clusters, enabling restores to known states. Dedicated clusters also support dual-region backups, which replicate approximately 99% of backup data to a secondary region within an hour to enhance cross-region disaster resilience. Additionally, Point-in-Time Restore (PITR) enables restoring to any prior timestamp, and Dedicated clusters require PITR to be explicitly enabled—all contributing to reduced Recovery Point Objectives, while TiDB's underlying architecture (Raft consensus, distributed replicas) ensures high availability and supports these robust recovery mechanisms.

Cluster Operation And Maintenance

The operation and maintenance of the TiDB cluster is undertaken by the ops operation and maintenance platform. The ops system manages and controls the operation and maintenance authorization process of the cluster. The granularity of permissions is controlled at the cluster level, and the Bastion bastion machine is used for cluster operation and maintenance. Bastion can more precisely control the permissions of operation and maintenance operations, supports restrictions on high-risk commands, and only allows operation and maintenance personnel to access authorized clusters. At the same time, in order to better control operation and maintenance personnel's access to user data plane clusters, in ops A new approval process has been added to the service to ensure that customers can be reasonably provided with better operation and maintenance services under the premise of data compliance. These measures will help improve data security while also complying with our higher requirements for customer data protection.



EVALUATE TiDB FOR YOURSELF

Start Your Free Trial

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