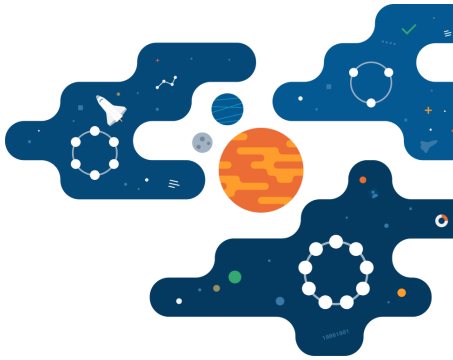
WHITEPAPER



DataStax Astra DB Security Overview

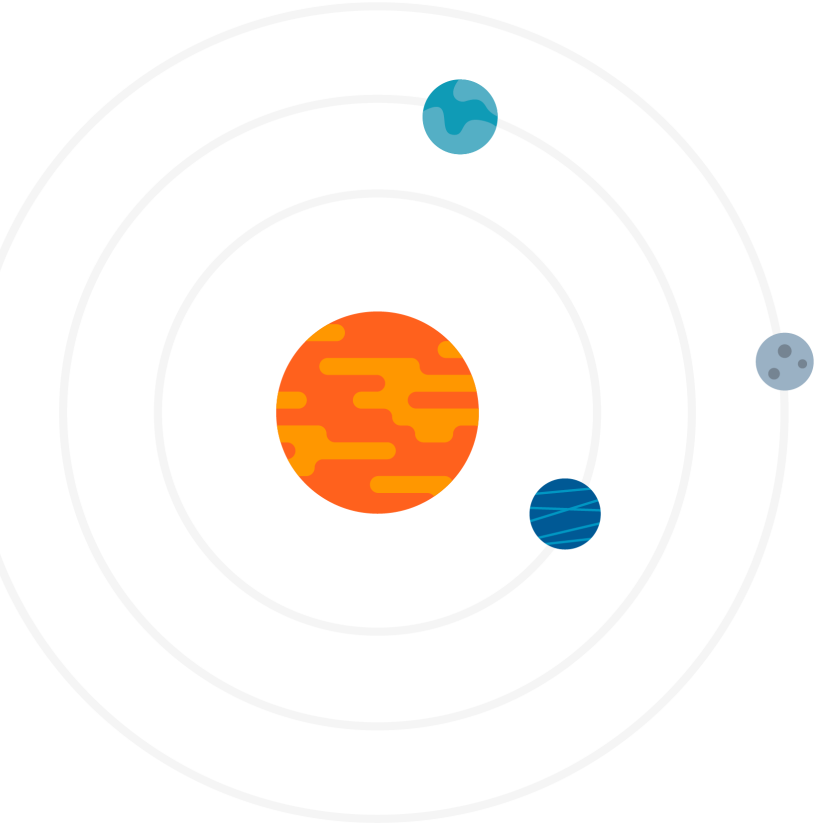
Serverless Database-as-a-Service with Enterprise-level Security and Privacy

DataStax Astra DB is the only open, multi-cloud, scalable, and serverless Database-as-a-Service. Built on Apache Cassandra™, DataStax Astra DB simplifies cloud-native application development, and reduces time to install, deploy and scale from weeks to minutes. Some of the benefits of using DataStax Astra DB:

- **Zero Operations.** DataStax Astra DB eliminates operational overhead, the biggest obstacle to using Apache Cassandra™, the open-source NoSQL database behind the largest applications in the world, including Netflix and Instagram. With DataStax Astra DB, enterprises can build secure, multi-cloud, multi-region applications with zero cloud vendor lock-in, zero-ops, and massively scalable database-as-a-service.
- **Developer Ready.** DataStax Astra DB makes it easy to add persistence and statefulness to modern applications. Native support for data APIs (via ***Stargate*** integration) enables your organization to get productive with Cassandra using REST, GraphQL, and schemaless Document APIs, without having to master CQL or NoSQL database concepts.
- **3x-5x Lower TCO (Total Cost of Ownership).** With serverless DataStax Astra DB, realize significantly reduced costs since you only pay for the compute, storage, or network capacity that you use, instead of sizing for peak and paying for unnecessary capacity that sits idle most of the time.

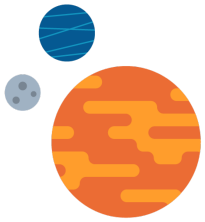
DataStax

- **Open and Multi-Cloud.** DataStax Astra DB is built on multiple Cloud Native Computing Foundation (CNCF) projects: Kubernetes, Prometheus, and Envoy and uses native GKE, AKS and EKS control and management planes with built-in management sidecars, metrics collectors, and configuration builders.
- **100% Uptime.** The DataStax Astra DB service is built on Cassandra and is, therefore, resilient and highly available to minimize both downtime and the need for additional site-reliability engineering. Replication is done across nodes in multiple zones/regions to ensure the highest possible availability.



01

Platform Security Features



DataStax Astra DB employs various strategies to ensure security and availability.

Secure Shared Infrastructure

DataStax user workloads are logically isolated within the ingest and processing components. Each database's data, backups, certificates and metadata are encrypted and stored in a dedicated bucket.

As a Database-as-a-Service offering, all Astra DB infrastructure -- the control plane, the Astra DB Console UI, and the database clusters are configured and operated within DataStax environments. The Astra DB control plane is built and purpose-hardened to reduce security vulnerabilities.

Intrusion Detection and Prevention

Astra DB uses a cloud-native Intrusion Detection System to monitor and protect against malicious and unauthorized access through custom log-based alerting and container scanning. When the Intrusion Detection System (IDS) alerts on irregular activity the Engineering and Security teams will investigate and resolve the alert.

VPC Peering

Select tiers of DataStax Astra DB support VPC Peering, which allows a user's personal or corporate-owned VPC to peer with the DataStax Astra DB VPC where the database runs. This ensures that the network connection between application clients and the database is entirely private. VPC peering is available for all cloud providers where DataStax Astra DB is offered.

Private Link & IP Access List

With Private Link, users have a private connection between VPCs, SaaS offerings such as DataStax Astra DB and their on-premises networks, without exposing database traffic to the public internet. Traffic between Astra DB and VPC stays on the cloud provider's network, reducing brute force and distributed denial-of-service attacks, along with other threats. Private link allows users to create private endpoints using global internal IP addresses for their VPC and eliminate the need to configure an Internet gateway, VPC peering connection, or manage VPC Classless Inter-Domain Routing (CIDRs)

With IP Access List, users can restrict access to Astra DB hosted endpoints by configuring access to specific IPs. Astra DB also supports the option to completely turn off public access if users choose to route all operations via private endpoints only.

Permission Log Audit

Audits are available for download with records of creation , deletion , and changes to custom roles, tokens, and users, up to the past 90 days.

02

Product Security Features

DataStax Astra DB includes capabilities that ensure confidentiality and data integrity.

End-to-End Encryption

Users connect to DataStax Astra DB via a secure endpoint that provides in-transit encryption via industry-standard mutually authenticated TLS (mTLS)—where both sides of the TLS connection use information in DataStax-generated certificates to verify the connection— with unique certificates created for each database cluster. DataStax continuously monitors the status of transport protocols, and requirements are continually updated in order to ensure weak ciphers are deprecated.

At rest, data is protected with the use of cloud native encryption for ephemeral and persistent datastores, in each cloud provider's respective object storage such as AWS Simple Storage Service (S3), GCP Cloud Storage, etc.

Role Based Access Control

DataStax implements role based access controls (RBAC) for client applications and users in Astra DB, where authorized access is granted based on role and the level of access is configured by customers based on need. Default roles are available to give varied levels of permissions within an organization, and custom roles can also be configured manually (via the Astra UI) or programmatically (via the DevOps API). With custom roles, permissions can be assigned for tokens or real users at the organization level, database level, keyspace level, and/or table level. Default roles are shown in table below:

Role	Permissions
Administrator User	Schema changes, including select, grant, modify, describe, authorize, drop for the tables and/or keyspaces for which the permission is granted Modify and describe keyspaces and tables within the database Select and describe keyspaces and tables within the database View databases in organization CQL access based on database access permissions GraphQL API access based on database access permissions REST and Document API access based on database access permissions Reset database password Park/unpark database
Organization Administrator	View billing Modify billing View users in an organization Modify users in an organization View databases in organization Create, terminate, and expand database VPC peering for database Reset database password Park/unpark database
Billing Administrator	View databases in organization View billing Modify billing
Database Administrator	View databases in organization Create, terminate, and expand database VPC peering for database Reset database password Park/unpark database
UI View Only	View databases in organization
Administrator Service Account	Schema changes, including select, grant, modify, describe, authorize, drop for the tables and/or keyspaces for which the permission is granted Modify and describe keyspaces and tables within the database Select and describe keyspaces and tables within the database CQL access based on database access permissions GraphQL API access based on database access permissions REST and Document API access based on database access permissions Reset database password Park/unpark database

Database, Keyspace, or Table Access Roles

Read/Write Service Account	Modify and describe keyspaces and tables within the database Select and describe keyspaces and tables within the database CQL access based on database access permissions GraphQL API access based on database access permissions REST and Document API access based on database access permissions
Read Only Service Account	Select and describe keyspaces and tables within the database CQL access based on database access permissions GraphQL API access based on database access permissions REST and Document API access based on database access permissions
Read/Write User	Modify and describe keyspaces and tables within the database Select and describe keyspaces and tables within the database View databases in organization CQL access based on database access permissions GraphQL API access based on database access permissions REST and Document API access based on database access permissions
Read Only User	Select and describe keyspaces and tables within the database View databases in organization CQL access based on database access permissions GraphQL API access based on database access permissions REST and Document API access based on database access permissions

API Access Roles

API Administrator User	Schema changes, including select, grant, modify, describe, authorize, drop for the tables and/or keyspaces for which the permission is granted Modify and describe keyspaces and tables within the database Select and describe keyspaces and tables within the database View databases in organization GraphQL API access based on database access permissions REST and Document API access based on database access permissions Reset database password Park/unpark database
API Read Only Service Account	Select and describe keyspaces and tables within the database GraphQL API access based on database access permissions REST and Document API access based on database access permissions

API Read/Write User	Modify and describe keyspaces and tables within the database Select and describe keyspaces and tables within the database View databases in organization GraphQL API access based on database access permissions REST and Document API access based on database access permissions
API Administrator Service Account	Schema changes, including select, grant, modify, describe, authorize, drop for the tables and/or keyspaces for which the permission is granted Modify and describe keyspaces and tables within the database Select and describe keyspaces and tables within the database GraphQL API access based on database access permissions REST and Document API access based on database access permissions Reset database password Park/unpark database
API Read/Write Service Account	Modify and describe keyspaces and tables within the database Select and describe keyspaces and tables within the database GraphQL API access based on database access permissions REST and Document API access based on database access permissions
API Read Only User	Select and describe keyspaces and tables within the database View databases in organization GraphQL API access based on database access permissions REST and Document API access based on database access permissions

Organization settings

In addition to role based access controls for database access, DataStax Astra DB offers organization level settings as an additional layer of security. The DataStax Astra UI enables administrative users to invite users from outside of their organization to collaborate. For example, this feature can be used to invite users from a different development team to participate on your team's project.

Developer Endpoints

REST, GraphQL, Document and DevOps API Endpoints

DataStax Astra DB offers endpoints for REST, GraphQL, and Document (JSON) APIs that can be used to perform operations against the database. Authorization for the developer endpoints is achieved by the generation of an application token.

TLS is used for all interactions with the DataStax Astra DB developer endpoints (see Encryption). Specific instructions on how to use the developer endpoints can be found in the ***developer endpoint documentation.***

Manage roles, users, tokens, and databases using DevOps API Endpoints

DataStax Astra DB offers developer endpoints that can be used to manage access to an organization, databases, keyspaces, or tables via a DevOps API. The DevOps API can also be used to programmatically create, view, park, resize, and terminate databases.

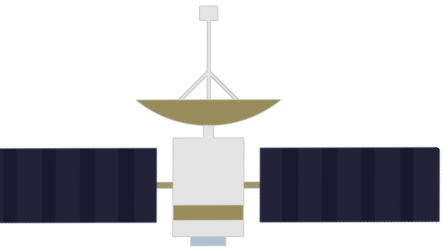
Access CQL endpoint using Secure Connect Bundle

The natively supported secure connect bundle streamlines the process for developers, administrators and service users to access the DataStax Astra DB through a CQL secure endpoint. The secure connect bundle contains the keys and certificates required for mutual authentication (mTLS), avoiding the need for the user to interact with them directly. It also contains the CQL configuration (cqlshrc) needed to connect to DataStax Astra DB from the CQL shell (cqlsh).

The secure connect bundle makes it easier to connect with DataStax Astra DB compared to a traditional, encrypted connection against Cassandra.

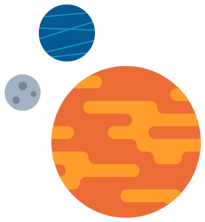
Client ID and Client Secret

When an application token is first generated, high entropy Client ID and Client Secret are also generated and displayed. These long-lived tokens allow client applications to be granted only the privileges necessary to an organization, specific databases, specific keyspaces, or specific tables by using custom roles. Client ID and Secret are available to copy or to download as a CSV file once only, at the time of token generation.



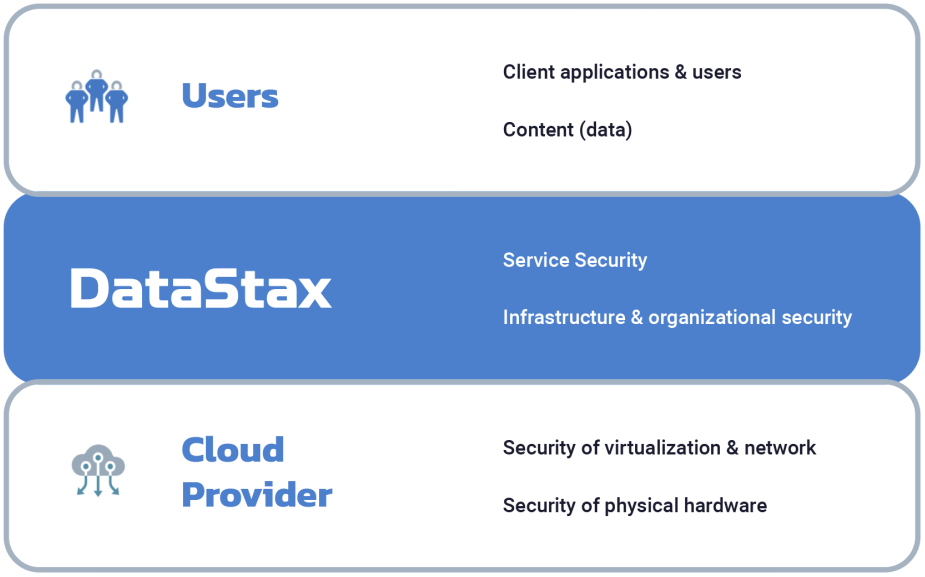
03

Shared Responsibility Model



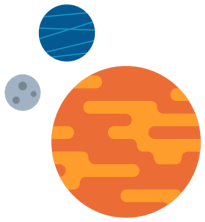
DataStax recognizes that a successful security framework in the cloud is understanding where one party's responsibility ends and the other's begins.

DataStax Astra DB users are responsible for the client applications, content and access via real users and networking settings. DataStax is responsible for the security of the service platform including the instance, operating system, DataStax Astra DB software and the relationship with the relevant cloud provider. The cloud infrastructure provider is responsible for the virtualization platform as well as the physical infrastructure and security of that infrastructure.



04

Compliance



DataStax follows global security standards and engineering and organizational best practices to weave security and privacy risk management traits into our DNA.

Industry Guidelines and Standards

In the effort to infuse security and privacy best practices into our development and operational routines, DataStax is informed by the following industry guidelines.

- **NIST 8000-53.** The National Institute of Standards and Technology (NIST) 800-53 CyberSecurity framework forms the basis of the program.
- **ISO 27001.** Information security management is informed by ISO 27001 best practices.
- **GDPR and CCPA.** Core privacy principles are based on the EU's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

DataStax is certified under the AICPA SOC2 framework. Reviews by external auditors affirm that controls are in place as of May 2020. The Type1 report is available under NDA as of late-June 2020 and the Type2 period ended on 31 January 2021, also available for review under NDA.

Organization Service Control Policies (SCPs)

The majority of operations performed on customer clusters are performed by software rather than staff. To the extent that manual operations are necessary, Service Control Policies (SCPs) provide guardrails against potential breaches:

- Staff access to production environments is granted by role with distinct privileges, following the principles of least privileged access
- Access to compute instances running customer clusters is restricted.
- Actions are logged and used for security monitoring.
- Logs are audited and used for automated alerts to detect unauthorized activities.

Incident Management

Incidents affecting the Astra DB service may be identified through a variety of sources, internal reporting, monitoring tools and customer submissions. DataStax maintains a documented Incident Management Policy and Incident Response Plan (IRP) which defines the process for triaging and resolving incidents. The IRP is tested annually to identify process improvements and to ensure internal stakeholders are aware of their responsibilities in the event of an incident. Any incidents affecting the Astra DB service are tracked through resolution by the Astra DB Engineering and Security teams.

Vulnerability Management

A vulnerability management program is in place that takes a holistic approach to identify, triage and remediate security risks based on severity and impact to the service. Vulnerability scanning, third-party penetration testing and a public vulnerability disclosure program form an integral part of addressing vulnerabilities:

- On a continuous basis, the internal DataStax security team tests and scans the Astra DB service against the latest known vulnerabilities to identify potential security risks.
- On a semi-annual basis, DataStax engages a third-party to conduct a penetration test to identify vulnerabilities in the service environment.
- DataStax uses a leading public platform for hosting an ongoing vulnerability disclosure to allow for researchers to report any findings that may present security flaws or potential data breaches. For more information on the vulnerability disclosure program, please visit: ***https://hackerone.com/datastax***

Third party risk management

A risk management process is in place to provide company personnel with guidance throughout the vendor lifecycle. Third parties are evaluated for security and privacy risks prior to onboarding and annually thereafter. As part of the evaluation, security documentation and contracts are obtained to evaluate for issues that may impact security, availability, confidentiality and privacy. Thereafter, third parties are evaluated on an annual basis using the same methodology.

Contractual arrangements are put in place with third parties to ensure that sufficient guarantees are in place to meet the requirements for secure processing found in privacy and data protection regulations around the world including the GDPR and CCPA.

Personnel Security Controls

Information security starts with the personnel that we employ throughout the employee lifecycle:

Prior to hire:

- Clearly defined roles and responsibilities are reviewed and approved within job descriptions
- Candidates are thoroughly evaluated based on role responsibilities and professional achievements.
- A thorough background check for all new hires is performed, as permitted by applicable law. The employee history checked will include criminal, employment, education, financial and credit checks as applicable for the role.

Upon hire:

- New hires sign proprietary information agreements or confidentiality clauses embedded within their employment contracts.
- New hires are required to undergo security awareness training and review all applicable security policies, processes and documentation.
- Access is granted based on principles of least privilege and requires management approval

During employment:

- Employees undergo regular security awareness training to address new and emerging risks in the cybersecurity domain.
- Periodic access reviews are conducted to ensure that access to environments is still appropriate.

Upon departure:

- All accounts, access privileges and physical assets are revoked and returned within pre-defined periods.

Engineering Best Practices

The DataStax Security & Compliance team is made an integral part of the Engineering organization. They ensure that information security and privacy protections are built in, by design, with a goal of making our products as secure as possible. All code is peer-reviewed, analyzed, tested and deployed through automation as part of DataStax's standard SDLC (Software Development Lifecycle).

Vulnerability Reporting

DataStax has a team of security experts and processes in place to support our customers whenever a security issue arises. An important strategy DataStax uses, in building secure applications, is to respond to vulnerability reports from our customers. DataStax employs the following process to handle vulnerability reports:

1. The reporter reports the vulnerability privately to DataStax via a support ticket.
2. The appropriate project's security team works to resolve the vulnerability.
3. DataStax Astra DB is patched.
4. DataStax Astra DB release notes will be updated to provide information on known and resolved issues and bug fixes after the patch has been made.

The Bottom Line: A Secure Database in the Cloud

DataStax is on the front line of security. Security practitioners can be confident in the depth of functionality, as well as the on-going investment in DataStax Astra DB. DataStax is continuously evolving Astra DB at a rapid pace to make it the easiest, and the most secure Cassandra-as-a-Service offering on the market.

© 2021 DataStax, All Rights Reserved. DataStax, Titan, and TitanDB are registered trademarks of DataStax, Inc. and its subsidiaries in the United States and/or other countries.

Apache, Apache Cassandra, and Cassandra are either registered trademarks or trademarks of the Apache Software Foundation or its subsidiaries in Canada, the United States, and/or other countries.