unify.USI

Unified Systems Intelligence

myunifyai.com

Security Protocols, Guides, and Technical/Organizational Security Measures

unify.PM unify.ATS

unify.SIGN unify.CRM

unify.SIS unify.HRM

unify.AMS

Table of Contents

Table of Contents

Table of Contents

Introduction

Building customer trust is a top priority at USI. USI adopts and utilized the MongoDB Atlas platform and security compliance standards as its security best practices. In this document, MongoDB Atlas is the sole owner of the overall content with USI leveraging the standards and outlines as best practices to its technology. We understand the responsibility we have when you, our customers, entrust us with a significant variety and amount of sensitive data. To maintain customer confidence in our security posture and in the security features we provide, we work diligently to continuously improve security processes and controls and provide our customers with the right features to secure the data. We take security seriously — from continuously fixing vulnerabilities and improving our security posture to enabling you to do just the same by providing various security features in our products. You will also find that we maintain and improve upon a full suite of security compliance certifications and attestations so as to keep up with the ever-changing threat and risk landscape.

At USI, we want you to have full confidence in the security and resiliency of the systems and technology that we maintain, and the products that we provide to facilitate secure growth and innovation in your company. We are hopeful that this document conveys the depth of our commitment to customer trust by providing a detailed understanding of Unify Systems security controls and features.

In addition to this document, we encourage you to review in the below sections the Technical and Organizational Security Measures. The security measures set out the security features, processes, and controls applicable to the cloud services, including configurable options available to customers, which employ industry standard information security best practices.

What is Unify Systems?

Unify Systems is built on MongoDB Atlas which is a fully managed cloud database with multi-cloud and multi-region data distribution capability. With automated infrastructure provisioning, database setup, maintenance, and version upgrades, customers can shift their focus to what really matters: building applications with speed and success. Atlas also comes with many drivers, tools, and a full suite of services (Atlas Search, Atlas Online Archive, Atlas Data Lake, and USI App Services) to help our customers build to new heights securely.

Unify Systems at a glance

Atlas provides a hierarchy based on organizations and projects to facilitate the management of your Atlas clusters. Multiple projects can exist within an organization. Billing happens at the organization level, though visibility into usage by the project is preserved.

By having multiple projects within an organization, you can:

- Isolate different environments from each other.
- Deploy into different regions or cloud platforms.
- Maintain separate cluster security configurations. For example:
  - Create/manage different sets of USI user credentials for each project.
  Isolate networks in different VPCs.
- Create different alert settings. For example, configure alerts for Production environments differently than Development environments.
- Associate different users or teams with different environments, or give different permissions to users in different environments.

-

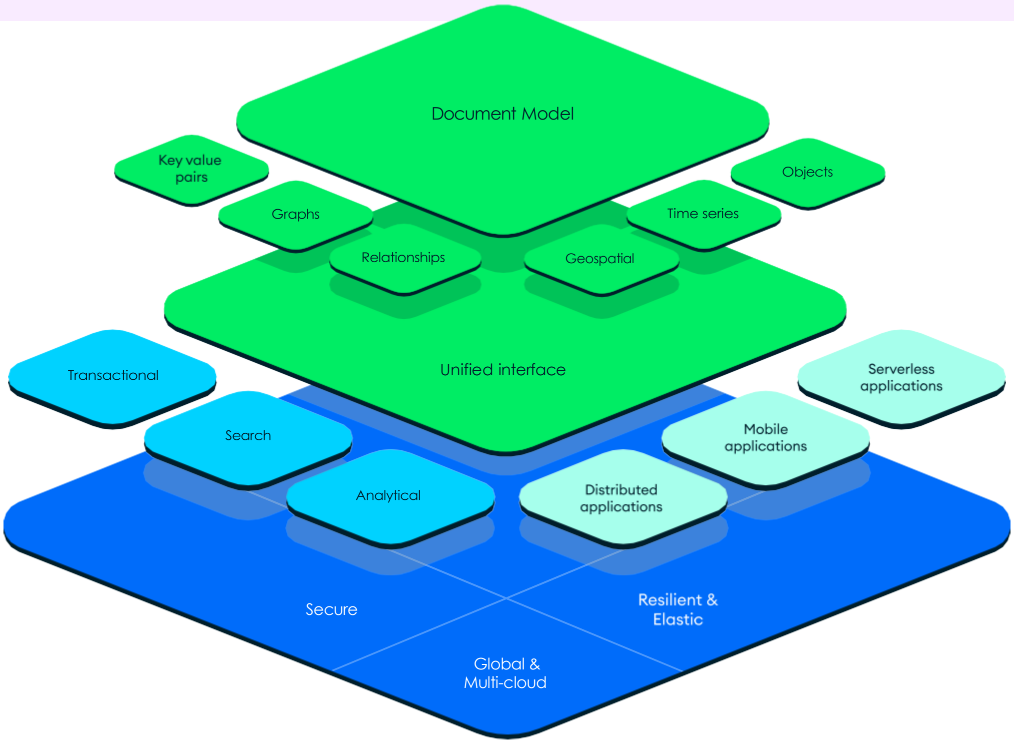


Figure 1. Unify Systems. The multi-cloud developer data platform

MongoDB Atlas Security Capabilities

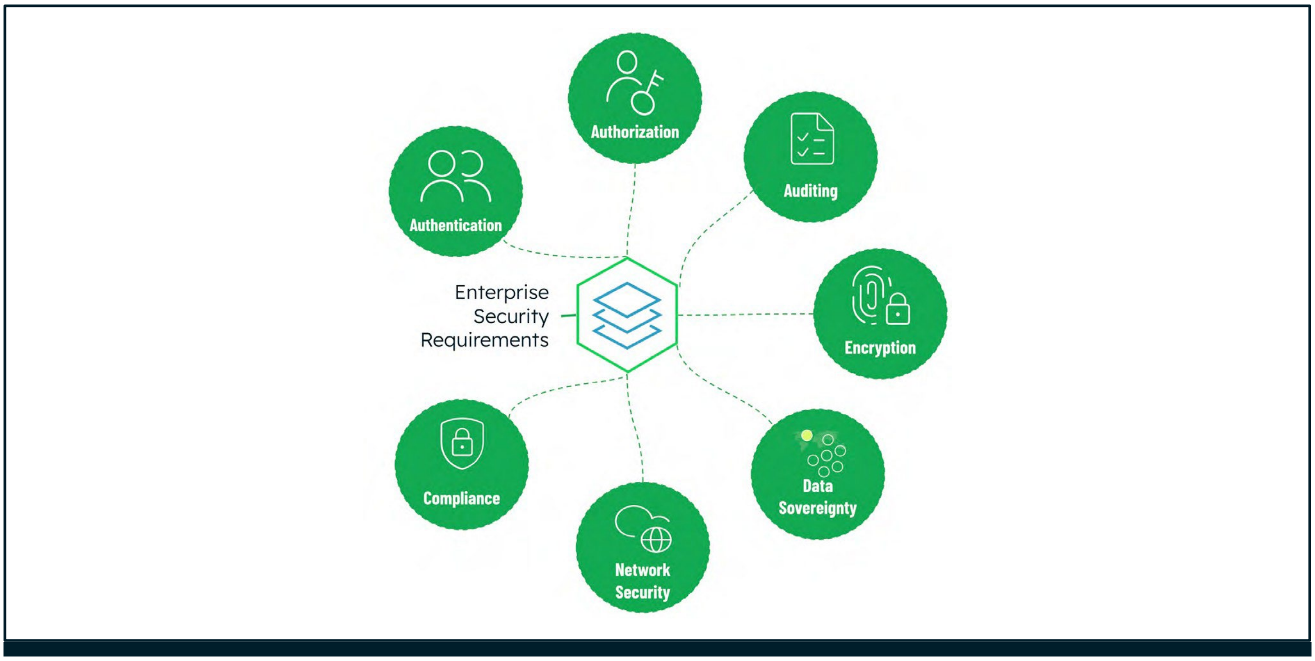


Figure 2. Unify Systems Security Capabililities

Unify Systems Security Capabilities at a glance	
Federated Authentication	Federated authentication using built-in integrations with Okta, Ping Identity, Azure AD, and others
Database Authentication	SCRAM, x509 certificates, AWS-IAM, LDAP
	Hashicorp Vault native integrations
Auditing	Always-on cloud user action and DB auth tracking
	Granular system activity tracking including DDL, DML, and DCL (Data Definition, Data Manipulation, and Data Control Language) commands
Encryption	Unify Systems integrates with your key management services of choice – AWS KMS, Azure Key Vault, Google Cloud KMS or any KMIP-enabled key provider
	Encryption in-use with client-side field level encryption technology
Data Sovereignty	Control data residency via cloud provider and 90+ region selection across AWS, Azure, & Google Cloud.
Network Security	IP Access lists, VPC Peering
	Private Endpoint (AWS, Google Private Service Connect, Azure Private link)
Compliance and Security Assurance	ISO 27001, 27017, 27018, CSA STAR II, SOC 2, HITRUST, PCI, VPAT, GDPR
	FedRAMP Moderate Authorized and CJIS (Unify Systems for Government)

Before we jump into details on each of the security capabilities listed above, let us quickly go through the Shared Responsibility Model.

Shared Responsibility Model

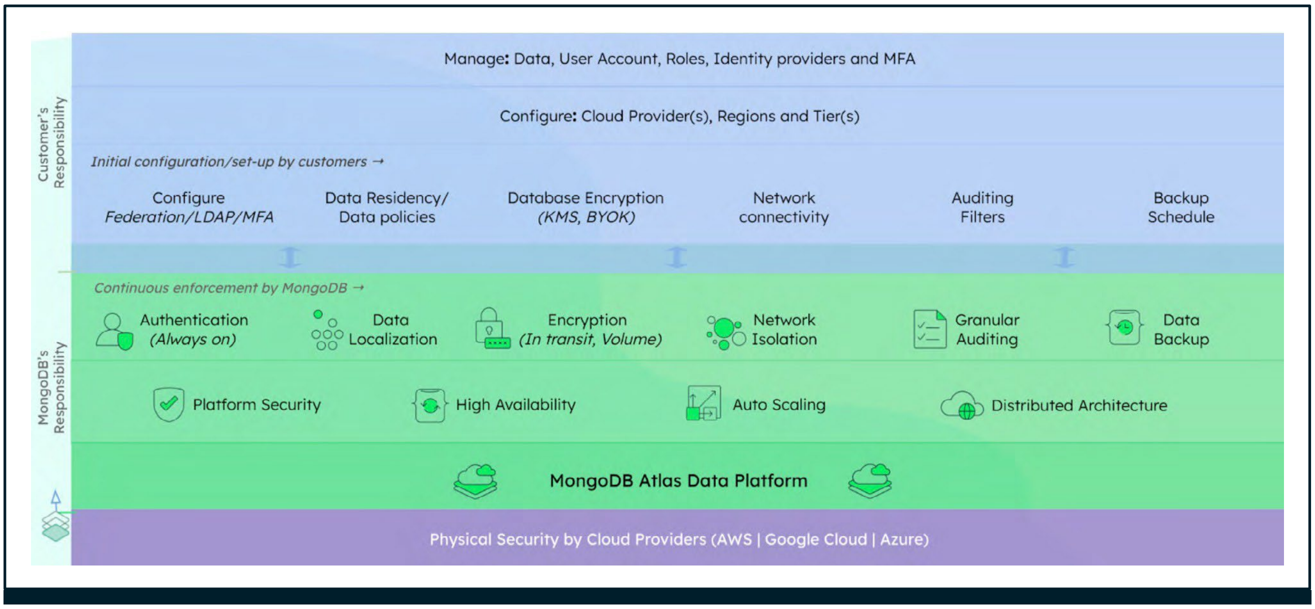

Customer's Responsibility
Manage: Data, User Account, Roles, Identity providers and MFA
Configure: Cloud Provider(s), Regions and Tier(s)
Initial configuration/set-up by customers →
Configure Federation/LDAP/MFA
Data Residency/ Data policies
Database Encryption (KMS, BYOK)
Network connectivity
Auditing Filters
Backup Schedule
MongoDB's Responsibility
Continuous enforcement by MongoDB →
Authentication (Always on)
Data Localization
Encryption (In transit, Volume)
Network Isolation
Granular Auditing
Data Backup
Platform Security
High Availability
Auto Scaling
Distributed Architecture
MongoDB Atlas Data Platform
Physical Security by Cloud Providers (AWS | Google Cloud | Azure)

Figure 3. The USI Shared Responsibility Model

As with any cloud service, the provider and customers share responsibility for securely using the service. Unify Systems has been designed with strong security defaults in mind so that the burden of securely using the service is minimized for the customer. These defaults include always-on authentication, authorization, encryption in transit, encryption at rest, and no database access from the internet by default. Unify Systems is architected to provide automated database resilience and mitigate the downtime risks associated with hardware failures or unintended actions. For more in-depth information, read the Resilience and High Availability With Unify Systems whitepaper.

Customers are responsible for creating users and roles to access their Unify Systems databases, selecting cloud provider(s) and region(s) in which to create their clusters and the cluster type. They can optionally enable backup, configure advanced auditing, bring their own keys for storage engine encryption, and configure client-side field-level encryption.

For more details on the Shared Responsibility Model refer to the datasheet and the whitepaper.

Authentication and Authorization

Unify Systems supports multiple authentication and authorization options and methods to give customers the flexibility to meet their individualized requirements and needs. Unify Systems environment, which consists of a web application administrative interface (*Unify Systems UI*) and any Unify Systems Cluster you deploy. Unify Systems provides you with configurable authentication and authorization options for both the Unify Systems UI and your Unify Systems Clusters.

The Unify Systems Web UI/Control Plane is the web application where your administrators can manage Atlas clusters, including initial user and permissions setup. The Unify Systems UI/Control Plane supports authentication via username/ password and multi-factor authentication. Control plane user identities are managed in a USI-controlled instance, encrypted and stored securely. Federated identity with SAML identity providers such as Okta or Ping Identity are supported. Users may also create and login to an Atlas control plane account using a Google Account. Authentication to the Atlas UI/Control Plane times out after 12 hours; users will need to re-authenticate after that time. For the Unify Systems Cluster, authentication is automatically enabled by default to help ensure a secure system out of the box.

Unify Systems allows administrators to define permissions for a user or application, and what data can be accessed when querying USI. Unify Systems provides the ability to provision users with roles specific to a project or database, making it possible to realize a separation of duties between different entities accessing and managing the data.

Administrators can also create temporary USI users; Atlas will automatically delete the user after a specified period of time. This capability is highly complementary to granular database auditing (described in more detail below). For example, when a user needs to be granted temporary access to perform maintenance, the assigned role and all of its actions can be comprehensively audited. Once Atlas deletes the user, any client or application attempting to authenticate with the user will lose access to the database.

Multi-factor Authentication

For the Unify Systems Web UI, user credentials are stored using industry-standard and audited one-way hashing mechanisms. Additionally, customers can choose to optionally utilize multi-factor authentication, or require all of the users in their Atlas Organization to use multi-factor authentication. Multi-factor authentication options include SMS, voice call, a multi-factor app, or a multi-factor device (such as a YubiKey). Customer-sensitive data provided within the GUI, such as passwords, keys, and credentials that must be used as part of the service are stored encrypted.

x.509 Authentication

Ensure tighter security controls and adhere to existing security protocols by enabling passwordless authentication to Unify Systems clusters with X.509 certificates. Easily configure the X.509 option that works for your standards. X.509 is supported by two options "Easy" and "Advanced." Enable the "Easy" X.509 option in Unify Systems to auto-generate certificates to authenticate your database users. If you have pre-existing certificate management infrastructure you have the ability to enable the "Advanced" X.509 option to upload your CA certificate to Unify Systems and continue to use your in- house X.509 certificates for authentication. This option can be optionally combined with LDAPS for authorization. Atlas automates alerts when a certificate issued by the Atlas CA or CRL is close to expiration.

AWS IAM Authentication

Further simplifying cloud-native security, your applications, containers, and serverless functions can authenticate to Unify Systems clusters reusing existing regular and temporary AWS IAM credentials. Applications provisioned on EC2 instances, Docker containers managed by ECS, or serverless functions running on AWS Lambda can automatically obtain IAM credentials from local metadata, using them to authenticate to Unify Systems, just as you can for any AWS-native service. AWS IAM authentication is available only on clusters that use USI version 4.4 and higher.

AWS IAM authentication is available on all Atlas clusters, including those running on other cloud providers (Google Cloud, Azure).

LDAP Integration

User authentication and authorization against Unify Systems clusters can be managed via a customer's Lightweight Directory Access Protocol (LDAPS) server over TLS. A single LDAPS configuration applies to all database clusters within an Atlas project. For customers running their LDAPS server in an AWS Virtual Private Cloud (VPC), a peering connection is recommended between that environment and the VPC containing their Atlas databases.

API Access

For programmatic access to an organization or project, administrators can create organization-scoped API keys. As a prerequisite, you must turn on an organization-level setting that only allows programmatic API keys to be used if there is at least one API Access List entry. The creation and deletion of keys will be logged in the Atlas activity feed.

HashiCorp Vault Integration

You can use HashiCorp Vault to generate and manage secrets for Unify Systems database users and programmatic APs, standardizing and controlling workflows with other tools and services. Two Vault secrets engines manage the life-cycle of Atlas credentials that contain a secret: the *Unify Systems Secrets Engine* manages secrets for API keys, while the *Unify Systems Database Secrets Engine* manages database users.

Auditing

Control Plane Auditing

Atlas allows administrators to audit all events triggered from the Atlas UI at the Project or Organization level. The logs are available in the Atlas UI or the API.

Always-On Database Authentication Auditing

For dedicated clusters (M10 and above), Atlas provides an easy-to-read log of database authentication events — including both successes and failures — such as database user, source IP address, and timestamp. This can be accessed either within the Atlas UI or via the API.

Granular Database Auditing

Granular database auditing in Unify Systems allows administrators to answer detailed questions about systems activity by tracking all DDL, DML, and DCL commands against the database. All DML commands can be audited, including reads along with creations/updates/deletes. Admins can select the actions that they want to audit, as well as the USI users, Atlas roles, and LDAPS groups whose actions they wanted to be audited, right from the Atlas UI. A single auditing configuration applies to all database clusters within an Atlas project. When needed, audit logs can be downloaded in the UI or retrieved using the Unify Systems API.

Data Encryption

Data that is created, exchanged, and stored in an organization is one of its most valuable assets. Securing that data from compromise and unauthorized access, especially when it comes to personally identifiable information (PII), financial, health, or government information, should be at the very top of your priorities.

Authentication and authorization offer one level of security but your sensitive workloads which are critical to your organization has to be encrypted. USI encryption offers robust features, some coming out-of-the-box on the Unify Systems Data platform, which we will cover in this article.

Encryption in Transit

All Unify Systems network traffic is protected by Transport Layer Security (TLS), which is enabled by default and cannot be disabled. Customer data that is transmitted to Unify Systems, as well as customer data transmitted between nodes of your Unify Systems Cluster, is encrypted in transit using TLS. You can select which TLS version to use for your Unify Systems Clusters, with TLS 1.2 being the recommended default and a minimum key length of 128 bits.

Key management procedures for encryption in transit

All encryption in transit is supported by the use of OpenSSL FIPS Object Module. We maintain documented cryptography and key management guidelines for the secure transmission of customer Data, and we configure our TLS encryption key protocols and parameters accordingly. USI's key management procedures include:

1. Generation of keys with approved key length
2. Secure distribution, activation and storage, recovery and replacement, and update of keys
3. Recovery of keys that are lost, corrupted, or expired
4. Backup/archive of keys
5. Maintenance of key history
6. Allocation of defined key activation and deactivation dates
7. Restriction of key access to authorized individuals; and
8. Compliance with legal and regulatory requirements.

When a key is compromised, it is revoked, retired, and replaced to prevent further use (except for limited use of that compromised key to remove or verify protections). Keys are protected in storage by encryption and are stored separately from encrypted data. TLS certificates are obtained from a major, widely trusted third-party public certificate authority. In the course of standard TLS key negotiation for active sessions, ephemeral session keys are generated which are never persisted to disk, as per the design of the TLS protocol.

Encryption at Rest

Encryption at rest is a protection layer to guarantee that the written files or storage is only visible once decrypted by an authorized process/ application. Upon creation of a Unify Systems Cluster, by default, customer data is encrypted at rest using AES-256 to secure all volume (disk) data. That process is automated by the transparent disk encryption of your selected Cloud Provider, and the Cloud Provider fully manages the encryption keys. You may also choose to enable database-level encryption via the WiredTiger Encrypted Storage Engine (using AES-256), as well as to bring your own encryption key with AWS Key Management Service (KMS), GCP KMS, or Azure Key Vault.

- **Amazon Web Services**

  Encryption-at-rest is automated using AWS's transparent disk encryption, which uses industry standard AES-256 encryption to secure all volume (disk) data. All keys are fully managed by AWS.

  Customers running Unify Systems may also choose to optionally enable database-level encryption for sensitive workloads via the WiredTiger Encrypted Storage Engine. This option allows customers to use their own AWS KMS, Azure Key Vault, or Google Cloud KMS keys to control the keys used for encryption at rest. This capability is described in more detail below.

- **Microsoft Azure**

  Encryption for data at rest is automated using Azure's transparent disk encryption, which uses industry standard AES-256 encryption to secure all volume (disk) data. All keys are fully managed by Azure.

  Customers running Unify Systems may also choose to optionally enable database-level encryption for sensitive workloads via the WiredTiger Encrypted Storage Engine. This option allows customers to use their own AWS KMS, Azure Key Vault or Google Cloud. KMS keys to control the keys used for encryption at rest. This capability is described in more detail below.

- **Google Cloud**

  Encryption for data at rest is automated using Google Cloud's transparent disk encryption, which uses an Advanced Encryption Standard (AES) algorithm with a 256-bit key length, in Galois/Counter Mode (GCM). This is implemented in the BoringSSL library that Google maintains. In addition to the storage system level encryption, data is also encrypted at the storage device level with AES-256 on solid state drives (SSD), using a separate device-level key (a different key than the storage level). All keys are fully managed by Google Cloud.

Encryption at rest using Customer Key Management

Customers running Unify Systems may choose to "bring their own key" and enable database-level encryption for sensitive workloads via the WiredTiger Encrypted Storage Engine. All Atlas databases and snapshot backups use strong volume (disk) encryption by default to protect data at rest. The use of self-managed keys with the WiredTiger Encrypted Storage Engine can help customers achieve additional levels of confidentiality and data segmentation.

Please review the Atlas documentation on Encryption Key Management for the Encrypted Storage Engine for a general overview. The following describes how customers can delegate the use of their keys.

Atlas uses a customer's unique Master Key (AWS KMS Customer Master Key, Azure Key Vault Secret Key, or Google Cloud Service Account Key) per project to generate, encrypt, and decrypt its data master keys. Master keys are then used to encrypt database keys. This process is called envelope encryption.

Key Rotation

Customers who require key rotation can use Key Management Systems (KMS) and set the master key rotation policy for automatic rotation. Whether KMS or some other solution is integrated into the local key service (via, e.g., Hashicorp Vault, AWS Secrets Manager, Google Cloud KMS, or Azure Vault) we recommend that customers create IAM (Identity Access Management) profiles for access to those services, and make the scope very narrow — only encrypt/decrypt or retrieve/store for a single key or secret, and then rotate the identity keys/credentials to that IAM service account profile.

Customer Master Key

The Master Key in the context of a customer's cloud service – generates and decodes data keys. When the Encrypted Storage Engine is enabled for an Atlas project, customer databases can only be started or backed up when the customer's Master Key is active and valid.

Refer to the documentation, on how to manage the master key.

Encryption in use – Field Level Encryption

Unify Systems supports automatic encryption of individual data fields of Customer Data before they are sent to Unify Systems. If you enable this client-side field level encryption feature for a selected data field, an application-side component built into the USI drivers encrypts that field of Customer Data before leaving the driver to be sent to Unify Systems, and only decrypts it upon return to the application once inside the driver. With respect to the Customer Data for which you enable client-side field level encryption, Unify Systems never sees your unencrypted Customer Data and you control the encryption keys, which you can secure using any KMIP-compliant key management service.

Client-Side Field Level Encryption (FLE) provides among the strongest levels of data privacy and security for regulated workloads. What makes Client-Side Field Level Encryption different from other database encryption approaches is that the process is totally separate from the database server. Encryption and decryption are instead handled exclusively within the USI drivers in the client before sensitive data leaves the application.

USI's Client-Side FLE complements existing network and storage encryption to protect the most highly classified, sensitive fields of your records without:

- Developers needing to write additional, highly complex encryption logic
- Compromising your ability to query encrypted data
- Significantly impacting database performance

By securing data with Client-Side FLE you can move to managed services in the cloud with greater confidence. This is because the database only works with encrypted fields, and you control the encryption keys, rather than having the database provider manage the keys for you. This additional layer of security enforces an even finer-grained separation of duties between those who use the database and those who administer and manage the database.

You can also more easily comply with "right to erasure" mandates in modern privacy legislation such as the GDPR and the CCPA. When a user invokes their right to erasure, you simply destroy the associated field encryption key and the user's Personally Identifiable Information (PII) is rendered unreadable and irrecoverable to anyone.

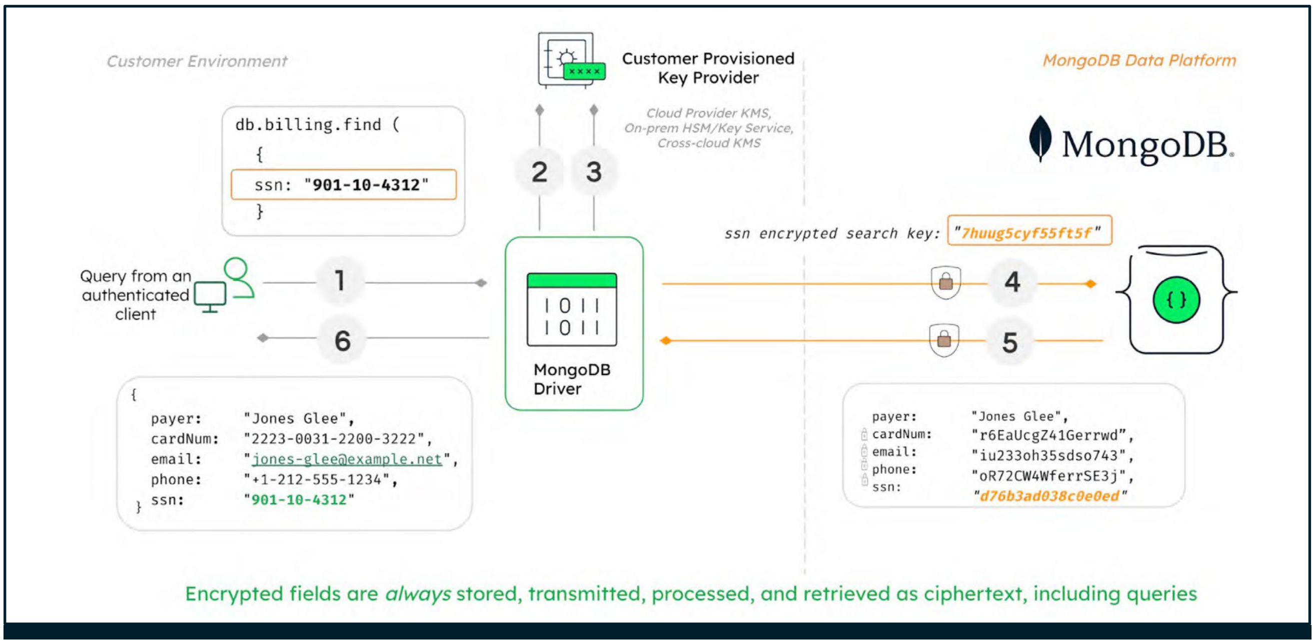
Client-Side FLE implementation

FLE is highly flexible. You can selectively encrypt individual fields within a document, multiple fields within the document, or the entire document. Each field can be optionally secured with its own key and decrypted seamlessly on the client.

Client-Side FLE uses standard NIST FIPS-certified encryption primitives including AES at the 256-bit security level, in authenticated CBC mode: AEAD AES-256-CBC encryption algorithm with HMAC-SHA-512 MAC.

Data encryption keys are protected by strong symmetric encryption with standard wrapping Key Encryption Keys, which can be natively integrated with external key management services backed by FIPS 140-2 validated Hardware Security Modules (HSMs). Client-Side FLE integrates with Amazon KMS, Azure Key Vault, Google Cloud KMS and any KMIP-compliant key manager. As an example, customers can use remote secure web services to consume an external key or secrets manager such as Hashicorp Vault.

To understand how FLE works in practice, let's take a look at the flow of a query submitted by an authenticated client, as shown in Figure 4.


Customer Environment
Customer Provisioned Key Provider
Cloud Provider KMS, On-prem HSM/Key Service, Cross-cloud KMS
MongoDB Data Platform
MongoDB.
Query from an authenticated client
1
2
3
4
5
6
MongoDB Driver
1011
1011
ssn encrypted search key: "7huug5cyf55ft5f"
{ }
Encrypted fields are *always* stored, transmitted, processed, and retrieved as ciphertext, including queries

```
db.billing.find (
  {
   ssn:  "901-10-4312"
  }
```

```
{
   payer:      "Jones Glee",
   cardNum:    "2223-0031-2200-3222",
   email:      "jones-glee@example.net",
   phone:      "+1-212-555-1234",
 } ssn:        "901-10-4312"
```

```
payer:         "Jones Glee",
cardNum:       "r6EaUcgZ41Gerrwd",
email:         "iu233oh35sdso743",
phone:         "oR72CW4WferrSE3j",
ssn:           "d76b3ad038c0e0ed"
```

Figure 4. USI Client-Side Field Level Encryption implementation

In this example we are retrieving a user's medical record by their SSN number:

1. When the application submits the query, the USI driver first analyzes it to determine if any encrypted fields are involved in the filter.
2. Recognizing that the query is against an encrypted field, the driver requests the fields' encryption key from the external key manager.
3. The key manager returns the keys to the USI driver, which then encrypts the ssn field.
4. The driver submits the query to the USI server with the encrypted fields rendered as ciphertext.
5. The USI server returns the encrypted results of the query to the driver.
6. The query results are decrypted with the keys held by the driver, and returned to the authenticated client as readable plaintext.

Note that in the query flow, the raw key material is never persisted to disk. Rather it resides only in memory on the application server, never accessed by or transmitted to the database.

Since the database server has no access to the encryption keys, certain query operations such as sorts, regexes, and range-based queries on encrypted fields are not possible server-side. With this in mind, Client-Side FLE is best applied to selectively protect just those fields containing highly sensitive PII such as email addresses, phone numbers, credit card information or social security numbers. Reads against fields in the document that are not encrypted client-side will evaluate as normal, as part of any query or aggregation pipeline operation.

To learn more, download our guide to Client-Side FLE, and review these key resources:

- The Client-Side Field Level Encryption documentation provides more detail on the implementation of FLE. It covers supported encryption methods and algorithms; key management; schema enforcement, driver compatibility; and more.
- The Client-Side FLE tutorial provides worked examples in multiple languages for full stack developers using a healthcare application as an example.

Data Sovereignty

Data Sovereignty is the idea that data are subject to the laws and governance structures of the region where they are collected. The concept of data sovereignty is closely linked with data residency, data security, cloud computing, network security, and technical controls. For example, what may be deemed as the acceptable use of personal information in one geography would not be so in some other region. To avoid data residency compliance issues, users need to conduct data mapping – that is, understanding what data you have, where it's located, and the data residency policies for each respective location.

While data protection regulations such as GDPR, CCPA, HIPAA, PCI-DSS, and others stipulate requirements that are unique to specific regions, industries or applications, there are foundational requirements common across all of the directives, including:

- Physical storage of data in a particular geography or lack of explicit guidance.
- Restricting processing of data stored in a particular geography outside that geo.
- Restricting data access, enforced via user privileges and roles.
- The separation of duties when accessing and processing data.
- Recording user, administrative staff, and application activities with a database.
- Ability to remove personal data when requested.
- Measures to protect against accidental or malicious disclosure, loss, destruction, or damage of personal data.

USI provides two mechanisms to meet with data sovereignty requirements:

1. **Dedicated USI clusters in a cloud provider and region of customer's choice**

   Ability to store data in any of the regions across AWS, Google Cloud and Azure as per your data locality requirements.

   Atlas databases are available in 90+ regions across AWS, Google Cloud, and Azure. You can even take advantage of multi-cloud and multi-region deployments, allowing you to target the providers and regions that best serve your users. Best-in-class automation and proven practices guarantee availability, scalability, and compliance with the most demanding data security and privacy standards. To support the data sovereignty requirements of modern privacy regulations, USI zones allow precise control over where personal data is physically stored in a cluster. Zones can be configured to automatically "shard" (partition) the data based on the user's location — for example enabling administrators to isolate personal data to just countries in the EU. If a company or regulatory policies towards storing data in specific regions change, updating the shard key range enables the database to automatically migrate personal data to alternative regions. With Unify Systems, you can control your data residency the way you desire – Single region or multi-regions and Single cloud or multi-cloud deployments.

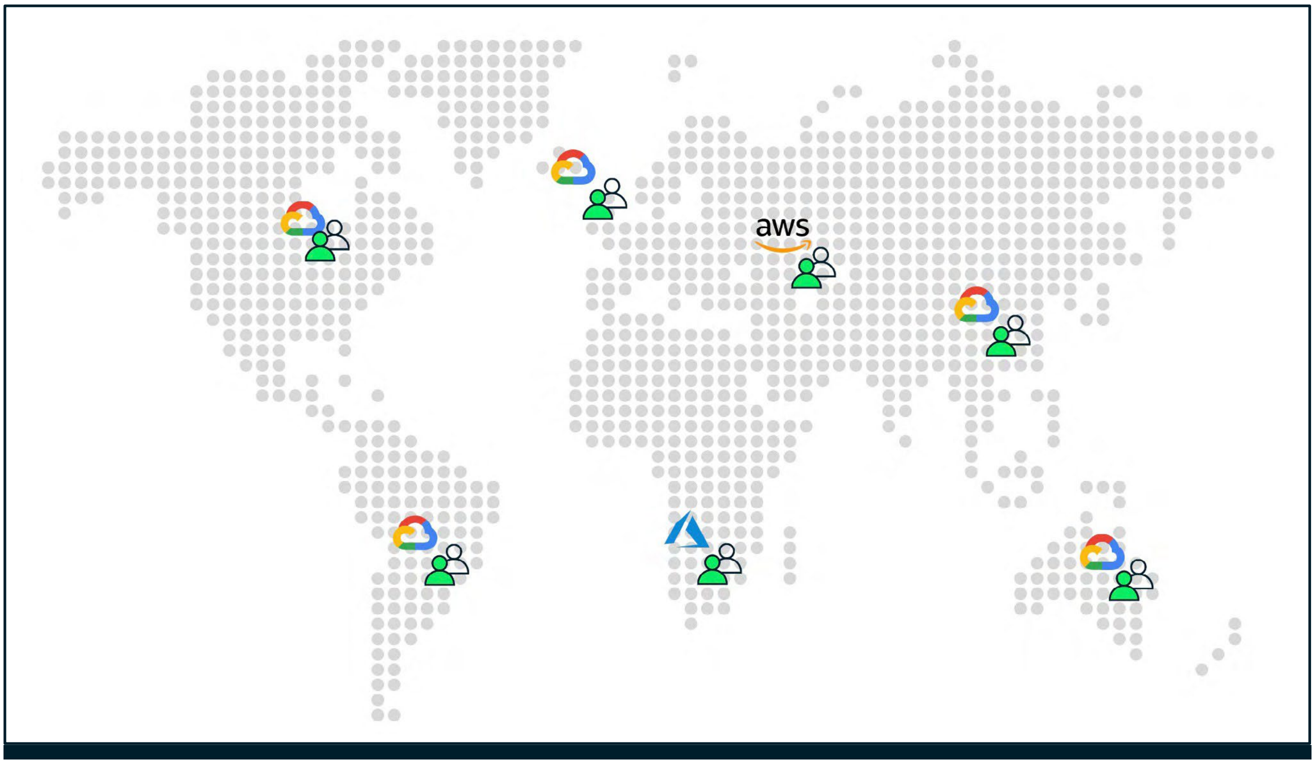


Figure 5. Unify Systems Clusters can be spread across many regions

2. **Global clusters with zoned sharding**

Zoned sharding is available to Unify Systems customers as part of the Global Clusters that are fully-managed cloud service providing a highly curated implementation of zoned sharding to support location-aware storage and database operations for globally distributed application instances and clients. For more information on global clusters refer to the documentation.

In addition, USI offers strict security controls with features discussed above like authentication, authorization, auditing, encryption, and network security along with proactive monitoring of our platform. All of this help to support customers' data residency requirements.

Unify Systems undergoes independent verification of platform security, privacy, and compliance controls. From the perspective of the GDPR, Unify Systems is GDPR compliant. USI and the Atlas service is classified as data processor. USI's terms of service reflect the GDPR's requirements, whereby we implement the appropriate technical and organizational measures in such a manner that processing will meet Regulation requirements and protect against destruction, loss, alteration, and unauthorized disclosure or access to personal data. You can learn more about Unify Systems GDPR compliance from the USI trust center.

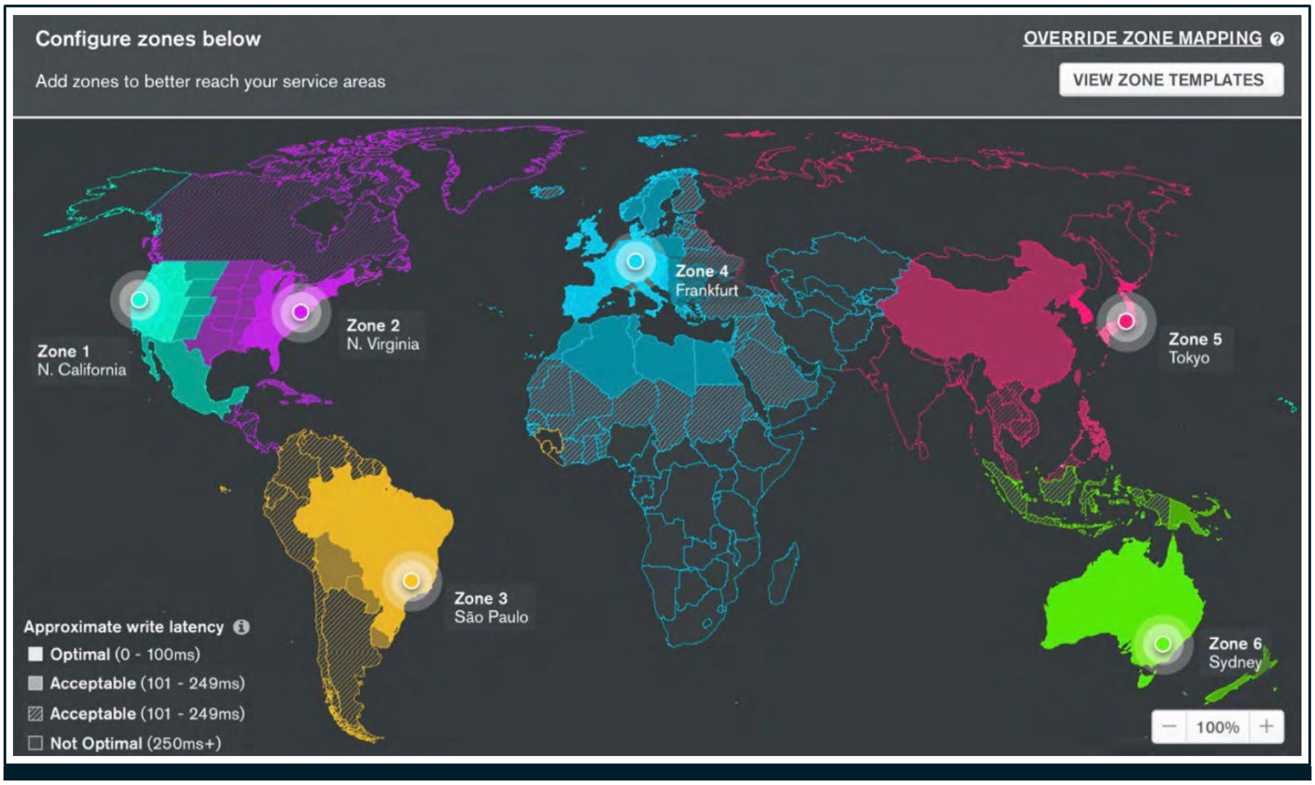


Figure 6. Unify Systems Global Clusters with Zoned Sharding

Network Security

Connectivity

USI requires the following network ports for Atlas. Network ports cannot be changed.

- 27017 for mongod (database server)
- 27016 for mongos (query router for sharded clusters)
- 27015 for the BI connector
- If LDAPS is enabled, USI requires LDAPS network port 636 on the customer side open to inbound traffic by Atlas

For detail configuration settings, please refer to the network and firewall settings.

You can connect to Atlas via either public IPs (which are protected with IP Access Lists, discussed below) or private IPs (via network peering or private endpoints, discussed below). Connection method for public vs. private IPs varies between cloud providers, as discussed in the following sections.

Atlas cluster public IPs remain the same in the majority of cases of cluster changes: vertical scaling, topology changes, maintenance events, healing events, etc. However, certain topology changes – such as a conversion from a replica set to a sharded cluster, an addition of shards, or a region change – will require new IP addresses to be used.

IP Access Lists

By default, your Unify Systems cluster will have no database access from the internet. Each Atlas cluster is deployed within a VPC configured to allow no inbound access by default.

Customers can configure IP Access Lists to limit which IP addresses can attempt to authenticate to their database. Application servers are prevented from accessing the database unless their IP addresses (or a CIDR covering their IP addresses) have been added to the IP Access List for the appropriate Unify Systems project.

Atlas also supports creating temporary access list entries that automatically expire within a user-configurable period. This can be useful in situations when a member of the team needs access to an environment from a temporary work location.

As a general best practice to reduce the attack surface, USI recommends customers only permit IP access to the smallest network segments possible (e.g., individual /32 address), and to avoid overly large CIDR blocks.

Network Peering

Network peering allows you to connect your own VPCs with an Atlas VPC, routing traffic privately and remaining isolated from the public internet. When you set up network peering, you can choose to only enable access via private IP from the peered network(s), or also allow access via public IP (controlled by the IP Access List).

Atlas does not need access into peered VPCs except when LDAPS is enabled. In that scenario, Atlas clusters need to reach the customer's LDAPS directory inside their VPC using the LDAPS protocol.

Customers worried about peering extending the network trust boundary to their dedicated Atlas-side VPCs can set up mitigating controls, including security groups and network ACLs, to not allow any inbound access to instances in their VPC from the Atlas-side VPC.

Customers with legacy VPCs internally that contain a large amount of infrastructure without isolation may be particularly uncomfortable introducing VPC peering and associated access governance. These customers should deploy net new VPCs for the applications requiring access to Atlas, isolating resources from each other within their own organizational network. These new VPCs can in turn be peered with the legacy/central VPCs.

Applications inside of such a VPC can reach both Atlas and other internal services but since VPC peering is non-transitive, Atlas cannot reach beyond the directly peered VPC — i.e., Atlas cannot reach your central VPCs. AWS Transit Gateway and AWS Direct Connect do provide transitive connectivity, so customers using AWS PrivateLink can use Transit Gateway or Direct Connect with your VPC to connect to Atlas via AWS PrivateLink (FAQ).

Private Endpoints

This connection method uses a one-way connection from your own VPC to the Atlas VPC. Atlas VPCs can't initiate connections back to your VPCs, ensuring that your network trust boundary is not extended.

Connections to private endpoints within your VPC can be made transitively from:

- Another VPC peered to the private endpoint-connected VPC.
- An on-premises data center connected with DirectConnect to the private endpoint-connected VPC.

Private endpoints are available on:

- AWS via AWS PrivateLink
- Azure via Azure Private Link
- Google Cloud via Private Service Connect

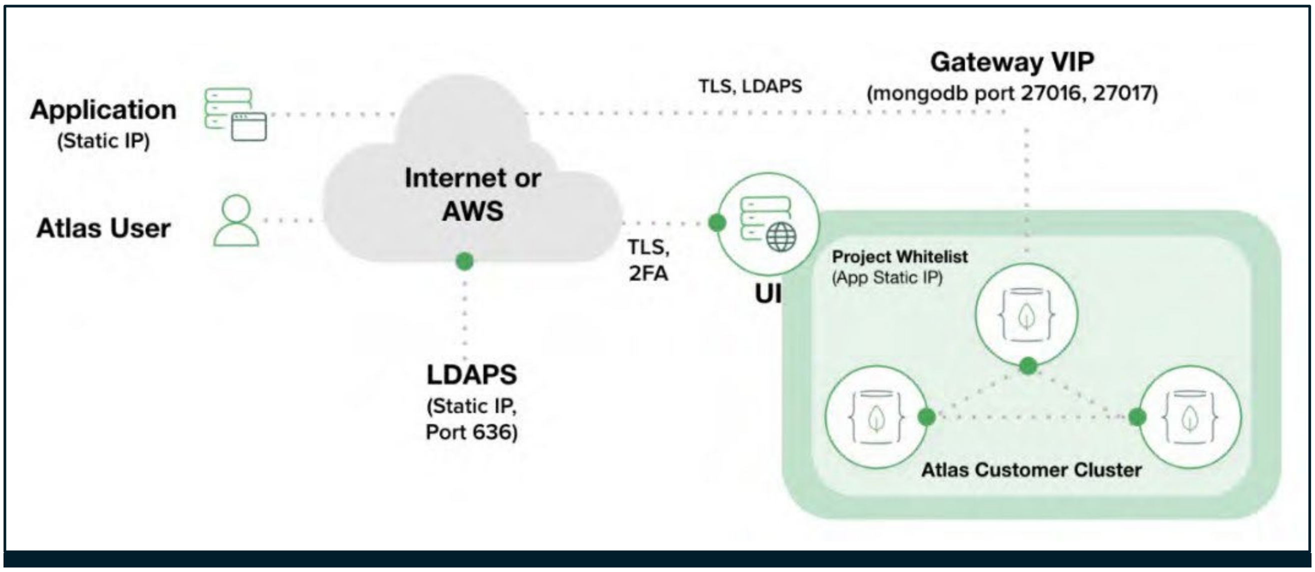
AWS VPC Topology

This section helps you review common practices to securely connect your individual clients to a Unify Systems service running in an Amazon Web Services Virtual Private Cloud (VPC).

Atlas deploys a cluster in a dedicated AWS VPC and then uses authentication and the IP Access List to isolate the service. On AWS, a cross-region cluster will span multiple VPCs and an Atlas project with clusters in different regions will be using a VPC per region.

If leveraging VPC peering, the AWS VPC resolves hostnames in an Atlas cluster to their private IP addresses when you enable DNS resolution. You can use these DNS entries to connect to hosts in your Atlas cluster from the peered VPC since AWS handles resolving the peered hostnames automatically.

Single-region VPC peering connections enable Atlas to reference security groups in the peered VPC by security group ID. Atlas also supports leveraging cross-region VPC peering connections. When doing so, it is not possible to reference security groups in a peered VPC on the Atlas Access List.



Customers leveraging custom DNS solutions that cannot take advantage of built-in split-horizon DNS may enable a project setting that provides a connection string that will resolve only to private IPs.

An additional networking option for AWS is AWS PrivateLink. With PrivateLink, Atlas clusters cannot initiate connections back to your application VPC, preserving your network trust boundary and reducing your security risk. AWS PrivateLink simplifies your network architecture by allowing you to use the same set of security controls across your organization. It also provides transitive connectivity from other peered and Direct Connect contexts, allowing you to connect to Atlas locally and from on-prem data centers without using public IPs via the IP Access List.

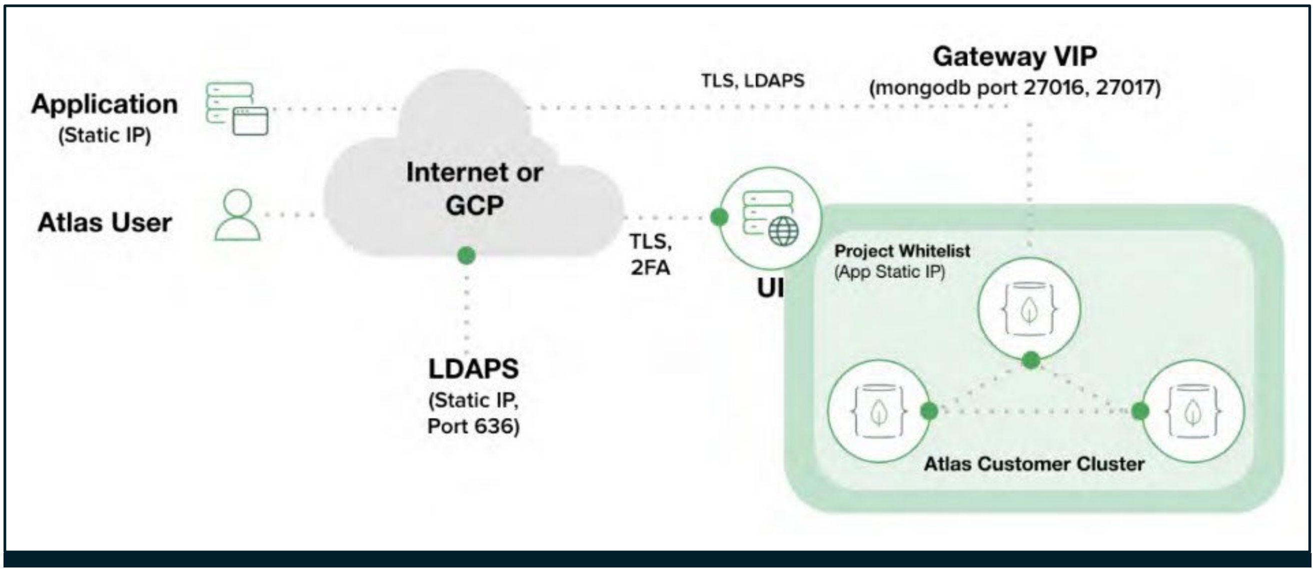
Google Cloud VPC Topology

This section helps you review common practices to securely connect your individual clients to a Unify Systems service running in a Google Cloud VPC.

Atlas deploys a cluster in a dedicated global Google Cloud VPC and then uses authentication and the IP Access List to isolate the service. A logical service in Google Cloud has its DNS name registered upon creation. The DNS name points to a gateway virtual IP (VIP) address in the datacenter where the service was created. Your individual application client needs a static IP assigned, which gets added to the project access list in Atlas.

VPC peering is available for Unify Systems deployments on Google Cloud. Once enabled, users can choose to connect to their Unify Systems cluster either with public IPs added to the Access List or VPC peering connections.

On Google Cloud, a cross-region cluster will use a single VPC, and an Atlas project with clusters in different regions will also use a single VPC.

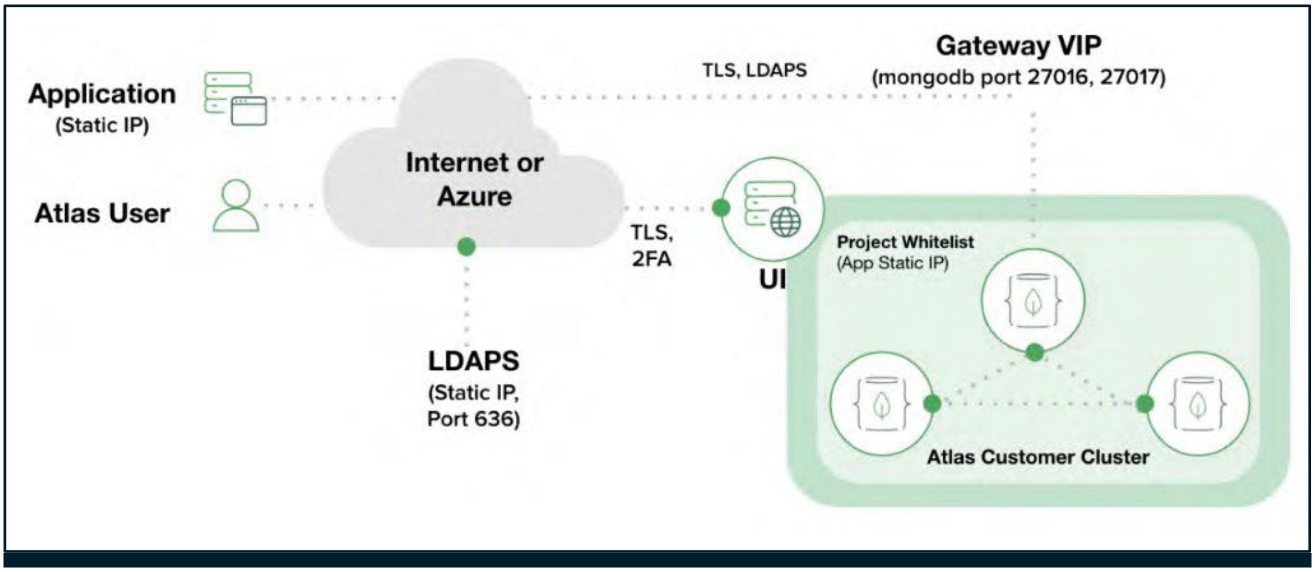


Microsoft Azure VNET Topology

This section helps you review common practices to securely connect your individual clients to a Unify Systems service running in an Azure Virtual Network (VNet).

Atlas deploys a cluster in a dedicated Azure VNet and then uses authentication and the IP Access List to isolate the service. A logical service in Microsoft Azure has its DNS name registered upon creation. The DNS name points to a gateway virtual IP (VIP) address in the datacenter where the service was created. Your individual application client needs a static IP assigned, which gets added to the project access list in Atlas.

On Azure, a cross-region cluster will span multiple VNets and an Atlas project with clusters in different regions will be using a VNet per region.



VNet peering is available for Unify Systems deployments on Azure, for both the single region and multi-region clusters. Once enabled, users can choose to connect to their cluster either with public IPs via the Access List or VNet peering connections.

An additional networking option for Azure is Azure Private Link. With Private Link, Atlas clusters cannot initiate connections back to your application VNet, preserving your network trust boundary and reducing your security risk. Azure Private Link simplifies your network architecture by allowing you to use the same set of security controls across your organization. It also provides transitive connectivity from other peered and ExpressRoute contexts, allowing you to connect to Atlas locally and from on-prem data centers without using public IPs via the IP Access List.

Compliance & Trust

USI has a comprehensive compliance & trust program for its cloud offerings. USI is committed to delivering the highest levels of standards conformance and regulatory compliance as part of our ongoing mission to address the most demanding security and privacy requirements of our customers.

Unify Systems Compliance

The scope of services under compliance and trust includes Atlas Database, Atlas Search, Atlas Data Lake, Charts, USI Realm, Cloud Manager, and USI Serverless.

ISO 27001

The ISO/IEC 27001 family of standards is designed to help manage the global security of assets such as financial information, intellectual property, employee details or information entrusted to a service provider. Today there are more than a dozen 27000 family standards. 27001 sets requirements for an information security management system (ISMS). USI cloud services has achieved ISO/IEC 27001:2013 certification. Learn More.

ISO 27017

ISO/IEC 27017:2015 provides guidance and recommendations of implementing cloud-specific information security controls that supplement the ISO/IEC 27001 standards, to ensure continuous management of security in a comprehensive manner. Learn More.

ISO 27018

ISO/IEC 27018:2019 is one of the critical components of cloud security – protecting data. There is sensitive data on the cloud, especially personally identifiable information (PII), company proprietary, and other sensitive data which is important to protect for organizations. ISO 27018 standard focuses on security controls that are built upon existing ISO/IEC 27002 security controls and provides new controls for personal data protection. Learn More.

SOC 2

Service Organization Controls (SOC) framework establishes a standard for controls that safeguard the confidentiality and privacy of information stored and processed in the cloud. Unify Systems is audited at least annually against the SOC reporting framework by independent third-party auditors. The audit covers controls for data security; the report is available to customers who've signed an NDA with USI, Inc. Learn More.

PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) applies to all entities that store, process, and/or transmit cardholder data. Unify Systems has been validated as a PCI compliant service provider by an independent Qualified Security Assessor (QSA). Customers are still responsible for managing the security of their own PCI DSS certification as well as configuring their Unify Systems deployments to comply with their PCI DSS requirements. Learn More.

HIPAA

For customers who are subject to the requirements of the Health Insurance Portability and Accountability Act of 1996, Unify Systems supports HIPAA compliance and enables covered entities and their business associates to use a secure Unify Systems environment to process, maintain, and store protected health information. USI, Inc. will enter into Business Associate Agreements covering Unify Systems with customers as necessary under HIPAA. Learn More.

HITRUST

USI maintains a SOC 2 + HITRUST certification report, mapping USI's SOC 2 Type II controls to the 75 required HITRUST controls for certification. Mapping requirements between SOC 2 and HITRUST is an approach recommended by both AICPA (SOC) and HITRUST. Learn More.

GDPR

The General Data Protection Regulation (GDPR) standardizes data protection law across all 28 EU countries and imposes strict new rules on controlling and processing personally identifiable information. The terms of service applicable to Unify Systems automatically include data processing protections that satisfy the requirements that the GDPR imposes on data controllers' relationships to data processors. Learn More.

CSA STAR

USI has achieved CSA STAR Level 2, via a third-party audit of Atlas's security. The CSA Security, Trust, Assurance, and Risk (STAR) Registry is a publicly accessible registry that documents the security and privacy controls provided by popular cloud computing offerings. STAR encompasses the key principles of transparency, rigorous auditing, and harmonization of standards outlined in the CSA's Cloud Controls Matrix (CCM). Learn More.

VPAT

USI has issued Accessibility Conformance Reports based on VPAT for Unify Systems, Unify Systems for Government, and the USI database software. Download USI's VPAT reports. Learn More.

Unify Systems for Government Compliance

FedRAMP® authorized and dedicated environment of Unify Systems for the US public sector as well as ISVs looking to build offerings for the US public sector.

FedRAMP® Moderate Authorized

FedRAMP® is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. Unify Systems for Government is FedRAMP Moderate Authorized. Atlas for Government is an independent, dedicated environment for the US public sector, as well as ISVs looking to build US public sector offerings. This platform is operated by USI employees who are U.S persons on U.S soil – is an integrated set of data and application services that share a unified developer experience – supports a wide range of use cases including transactional workloads, time series data, search, and petabyte data storage. Learn More. Documentation.

Criminal Justice Information Solutions (CJIS)

There is no standardized accreditation or assessment for CJIS compliance. There are set security standards and controls laid out in the CJIS Security Policy and USI is committed to helping customers meet those requirements. Additionally, USI engaged an independent auditor to evaluate how Unify Systems for Government (US) aligns with CJIS requirements. This attestation letter is available to customers subject to CJIS requirements by request. Learn More.

Business Continuity and Disaster Recovery

USI maintains a formal business continuity and disaster recovery process which covers its RTO[1] and RPO[2] ith regard to its Atlas control plane, and the supporting infrastructure of customer clusters in Atlas including VMs, DNS, and logs.

The Atlas control plane is the controller that provisions USI clusters in one or more regions as requested by the customers. Once the Atlas control plane creates USI database clusters, these clusters can continue to operate even if the control plane infrastructure is offline. If the supporting infrastructure of customer clusters is unavailable, customer connectivity to Atlas clusters may be impaired (e.g., due to DNS name resolution failure), or certain functionality may be impaired (e.g., storing and downloading logs).

How can you achieve your own business continuity objectives with Unify Systems?

Customers have a responsibility to maintain their own business continuity/disaster recovery and define their own RTO[1]/RPO[2] values according to their acceptable criteria (e.g., RTO/RPO of 0-4 hours), which can be achieved independently of the Unify Systems control plane RTO/RPO, via the use of specific product features available to customers. These features include:

- Selection of the underlying cloud provider(s) — AWS, Google Cloud, Azure — for deploying USI clusters, in order to mitigate the risk of a cloud provider failure.
- Selection of one or more cloud provider(s) regions, in order to mitigate the risk of a region failure.
- Selection of a clustered tier — shared or dedicated, sharded or unsharded — to mitigate the impact of workload spikes.
- Selection of network connectivity options to Atlas for high availability.
- Selection of backup & restore options and the backup schedule.

Infrastructure Service Recovery

Unify Systems creates and configures dedicated clusters on infrastructure provided by AWS, Azure and/or Google Cloud. Data availability also is subject to the infrastructure provider service Business Continuity Plans (BCP) and Disaster Recovery (DR) processes. Our infrastructure service providers hold a number of certifications and audit reports for these controls. For more information, please see below:

- Amazon Web Services Compliance
- Microsoft Azure Compliance
- Google Cloud Compliance

[1] RTO: Recovery Time Objective—describes how long it will take to get an application back online

[2] RPO: A Recovery Point Objective—is the maximum amount of data that can be lost before causing detrimental harm to the organization

Cloud Backup

Available for Atlas clusters deployed in Amazon Web Services, Microsoft Azure, and Google Cloud, cloud provider snapshots use the native snapshot capabilities of the underlying cloud provider.

Backups are stored in the same cloud region as the corresponding cluster. For multi-region clusters, snapshots are stored in the cluster's preferred region. All managed snapshots and images are automatically encrypted. If the encryption key management integration with AWS KMS, Azure Key Vault, or Google Cloud KMS is enabled, your AWS Customer Master Key (CMK) /Azure Key Vault Secret Key / Google Cloud Service Account Key and IAM credentials are required to perform restores of backup snapshots. Cloud Backup enables you to customize the snapshot schedule and retention policies, with support for multi-year retention, making it easier for you to adhere to compliance obligations. An optional add-on, Continuous Cloud Backup, records the oplog for a configured window, permitting a restore to any point in time within that window and satisfying Recovery Point Objectives (RPOs) as low as 1 minute.

Incident Response

The Corporate Security team employs industry-standard diagnostic procedures to drive resolution during business-impacting events. Staff operators provide 24x7x365 coverage to detect incidents and manage the impact and resolution.

Resiliency Plans

USI's Corporate Security group has reviewed the USI resiliency plans, which are also periodically reviewed by members of the Senior Executive management team.

Support Coverage

For customers who have purchased an Atlas support plan, the USI Technical Services Engineering team provides support for the GA releases of the following software:

- USI Server
- USI Cloud Manager
- Unify Systems
- Unify Systems Search
- Unify Systems Data Lake
- USI Compass
- USI Charts
- USI Realm

Support is also provided to the tools and integrations pertaining to usage of the Atlas products including:

- USI Drivers
- USI Connectors, including BI and Spark
- Authentication/access controls to the Atlas clusters
- AWS, Azure, and Google Cloud integration related questions
- Performance
- Data Migrations

Platform – Infrastructure and Data Security

Unify Systems's infrastructure is designed to be fully automated via modern configuration management systems. Reducing human elements increases a security posture by reducing the chance for human error and making audit and alerting standardized. Unify Systems provisions Virtual Machines with hardened machine images built in-house, and all of our virtual servers are configuration-managed using Chef, which includes hardening steps. All systems run with a known set of running processes/components, which in turn is utilized for update/patching.

Separation of Production and Non-Production Environments

Unify Systems has a strict separation between production and non-production environments. Production and Customer data is never utilized for non-production purposes. Non-production environments are utilized for development, testing, and staging.

USI Policies require the principle of least privilege and separation of duties. As a result, developers are provided access to developer environments only and production environments are limited to personnel who have an operational need and appropriate authorizations.

Firewalls and Bastion Hosts

Unify Systems infrastructure is only accessible via bastion hosts. Bastion hosts are configured to require SSH keys (not passwords). Bastion hosts also require multi-factor authentication, and users must additionally be approved by senior management for backend access.

Logging and Alerting

USI maintains a centralized log management system for the collection, storage, and analysis of log data for production environments. This information is used for health monitoring, troubleshooting, and security purposes. Alerts are configured on systems in order to notify SREs of any operational concerns.

Log Retention

It is the policy of USI to retain its logs within its own infrastructure based on an Atlas Log Retention schedule. When the retention period is complete, logs may be destroyed. Except as otherwise indicated, logs shall be retained for the number of months or years indicated.

USI is to maintain complete, accurate, and high-quality logs in storage for the duration of the time periods provided in this document. The head of Atlas engineering is responsible for authorizing, overseeing, and ensuring that logs are maintained pursuant to this document.

No logs will be destroyed if they are relevant to a pending or threatened investigation of any matter within the jurisdiction of a federal department or agency, or any other official investigation.

Retention Schedule (minimum life)	**Log Source**
Six years	• Web Tier • Backup Tier • Splunk Audit/Query • AWS CloudTrail • OS /var/log/secure • DB events collection audit history
One year	• UI app • Backup app • Restore app • Backup service app
One month	• Customer's USI • (mongod) and audit logs • Server Automation Agent • Server Backup Agent • Server Monitoring Agent • Data "mirror" app

It is a crime for anyone to knowingly destroy logs with the intent to obstruct the proper administration of any investigation or proceeding under the jurisdiction of a federal department or agency. No logs will be destroyed if they are relevant to pending or threatened litigation matters when USI is a party in the case or expected to become a party or when USI has received a subpoena.

Secure Deletion of Data

If a customer terminates an Atlas cluster, the following happens: it will become unavailable immediately; USI, Inc. may retain a copy of the data for up to 5 days; the backup associated with the managed cluster is also terminated. If a customer terminates the backup, all snapshots become unavailable immediately. It may take up to 24 hours for all copies of the data to be deleted.

Input Validation

Input validation is done for data submitted to web applications, and verified with manual source code checks and peer reviews, as well as internal and external security team tests. Fuzz testing is also used for core product assessments.

Protection from Ransomware and Malware Attacks

One of the major concerns for enterprises today is the risk of data breaches and unauthorized exposure from ransomware. Primary vectors for malware/ransomware include malicious email, Windows AD networks, and compromised desktop browsers via infected websites. There are lot of mitigation strategies USI security features offer. First, there is a true end-to-end encryption – sensitive data is protected as the data remains encrypted from the client, during transport, while at rest in the database, and while being processed in memory. With elevated features like Client Side Field Level Encryption, there is never any cleartext available in the database for sensitive workloads, even to the highest privileged administrators or sysadmins or cloud infrastructure staff and even if the database were to somehow get compromised by improperly secured credentials or some other exploit, hardened encryption technologies in use ensures that there is no data for an attacker to dump.

As part of the disaster recovery, by default Unify Systems offer an option to enable backups and customers can take backups as frequently as needed. In addition, by design all Atlas clusters are highly available, multi-node replica sets spanning multiple VMs, distributed regionally, globally, or even across multiple cloud providers. These backups can be targeted to multiple media target destinations and pulled to customer remote storage via automation or manually in the Atlas console at any time to authorized users.

Unify Systems offers additional safeguards depending on your business requirements and concerns.

- Customers can enable Termination Protection for clusters in Atlas, to ensure the prevention of accidental deletion of your production clusters and irretrievable loss of data by enabling cluster termination protection.
- Customers can also protect all of your backups as well. The Backup Compliance Policy enables organizations to further secure business-critical data by preventing all snapshots and oplogs stored in Atlas from being modified or deleted for a predefined retention period by any user, regardless of Atlas role, guaranteeing that backups are fully WORM compliant.
- With test failover in Atlas, you will be able to test the failure of a single node up to a regional failure at the click of a button to ensure you're ready for a real-life disaster event. Testing and ensuring your cluster's resiliency is working as you expect is no longer a one-time-a-year test but now just like your CI/CD process where you can continuously test your disaster recovery throughout the year at any time.

USI Personnel Access to Unify Systems Clusters.

Privileged user access

As a general matter, USI personnel do not have authorization to access your Unify Systems Clusters. Only a small group of Privileged Users are authorized to access your Unify Systems Clusters in rare cases where required to investigate and restore critical services. USI adheres to the principle of "least privilege" with respect to those Privileged Users, and any access is limited to the minimum time and extent necessary to repair the critical issue. Privileged Users may only access your Unify Systems Clusters via a gated process that uses a bastion host, requires MFA both to log in to our USI Systems and to establish a Secure Shell connection (SSH) via the bastion host, and requires approval by USI senior management.

Restricting USI personnel access

Unify Systems provides you with the option to entirely restrict access by all USI personnel, including Privileged Users, to your Unify Systems Clusters. If you choose to restrict such access and USI determines that access is necessary to resolve a particular support issue, USI must first request your permission and you may then decide whether to temporarily restore Privileged User access for up to 24 hours. You can revoke the temporary 24-hour access grant at any time. Enabling this restriction may result in increased time for the response and resolution of support issues and, as a result, may negatively impact the availability of your Unify Systems Clusters. If you enable client-side field level encryption, even Privileged Users will be unable to access Customer Data within your Unify Systems Clusters in the clear unless you provide USI with the encryption keys.

Credential requirements

Privileged User accounts may only be used for privileged activities, and Privileged Users must use a separate account to perform non-privileged activities. Privileged User accounts may not use shared credentials. The password requirements described in Section 4.3.3 also apply to Privileged User accounts.

Access review and auditing

USI reviews Privileged User access authorization on a quarterly basis. Additionally, we revoke a Privileged User's access when it is no longer needed, including within 24 hours of that Privileged User changing roles or leaving the company. We also log any access by USI personnel to your Unify Systems Clusters. Audit logs are retained for at least six years, and include a timestamp, actor, action, and output. USI utilizes a combination of automated and human reviews to scan those audit logs.

Dedicated Information Security Program

Security Program

USI maintains a comprehensive written Information Security Program to establish effective administrative, technical, and physical safeguards for Customer Data, and to identify, detect, protect against, respond to, and recover from security incidents. USI's Information Security Program complies with applicable Data Protection Laws and is aligned with the NIST Cyber Security Framework (NIST). Additionally, Unify Systems is certified against ISO 27001:2013, ISO 27017:2015, ISO 27018:2019, SOC 2 Type II, Payment Card Industry Data Security Standard v.3.2.1, and Cloud Security Alliance (CSA) Security, Trust, Assurance, and Risk (STAR) Level 2. Unify Systems has also undergone a HIPAA examination validated by a qualified third-party assessor and can be configured to build HIPAA compliant applications.

USI employees are required to take and attest to periodic security training. Additionally, the Security Team employs a number of education outreach efforts, such as internal security reading groups, Capture-the-Flag / Hacking Contests to teach developers security issues, hackathons, and more. Internal policies include data classification and handling and specific information regarding handling customer data.

USI has a vulnerability enumeration and management program; this program identifies internet-accessible company assets, scans for known vulnerabilities, evaluates risk, and tracks issue remediation. Vulnerability scans occur at least daily, with results reporting to a centralized security dashboard. A central company-wide ticketing system is used to track all security issues until remediation.

Human Resources performs multi-residence criminal background checks on all prospective employees. The HR employee off-boarding processes includes verification of account access termination.

Application Security

Unify Systems undergoes regular reviews from both internal and external security teams. Internally, Unify Systems undergoes periodic risk assessments, including technical vulnerability discovery and business risks and concerns.

Additionally, the USI Security Team is routinely involved in source code review, architecture review, code commit/peer review, and in security decision-making.

Application-level security testing uses a standard application assessment methodology (e.g., OWASP). Additionally, external engagements with security consults include social engineering and phishing testing. A summary of our most recent third-party penetration test is available for customers to review. Systems are patched as needed; security-related patches are applied commensurate to their severity.

Security Best Practices for Software Development

USI product security teams work collaboratively on security initiatives in the SDLC. Team members are tasked with finding and preventing security issues in our products. Their responsibilities include building new security features, reviewing source code, tracking and remediating security issues, and engaging with third parties for security reviews. All customer-facing software is in a continuous integration/delivery (CI/CD) pipeline and subjected to a peer-review process. We perform hundreds of hours of automated testing to ensure correctness on every source code commit. When code commit triggers (or "hooks") are called, unit tests and library integration links are automatically run, with a pass/fail log and real-time CI dashboard update. For more information on how we follow security best practices refer to the whitepaper.

Communication and Notifications

USI has an established Incident Response and Critical Communications Policy and associated processes. In the event that a security alert/event, or other signal results in USI declaring a security incident, USI will follow its internal incident response protocols and inform affected customers as soon as practicable. If your organization has very specific breach notification or communications requirements, please contact us directly.

Patching and Change Management

Patching of operating systems and applications are performed on a need-to-update basis. USI, Inc. employees utilize automated tooling in conjunction with monitoring security bulletins for relevant software and implement patches if security issues are discovered. The USI server software itself is continuously updated as new versions are released.

With respect to change management, development tasks are defined as issues for specific target releases. A release is deployed to production after it has transitioned through the requisite checkpoints, including testing, staged deployment, and management review. All internal release notes include a QA test plan.

Resources

We are USI, database experts with over 40K+ customers relying on our commercial and cloud products/services. For more information, please visit USI.com or contact us at sales@USI.com.

Atlas Documentation

Unify Systems download

Case studies

USI Resource center

USI University (Free online training)

USI App Services

Unify Systems database as a service

USI Trust Center

Technical and Security Control Measures

Unify Systems for Government

FedRAMP Moderate Authorization (MongoDB Atlas for Government)

Criminal Justice Information Solutions

Cloud Shared Responsibility Model (Datasheet, Whitepaper)

Technical and Organizational Security Measures

These Technical and Organizational Security Measures (“Security Measures”) are incorporated into and form part of your applicable agreement with USI with respect to your use of USI Atlas (the “Agreement”). These Security Measures also apply to USI Atlas for Government, as modified by the USI Atlas for Government Addendum to the Agreement. Atlas refers to MongoDB Atlas. USI has adopted these technical and organization security measures as the standard compliance measures.

The Security Measures set out the security features, processes, and controls applicable to USI Atlas, including configurable options available to Customer, which employ industry standard information security best practices.

1. Definitions

The following terms have the following meanings when used in the Security Measures. Any capitalized terms that are not defined in the Security Measures have the meaning provided in your Agreement.

1.1. "Cloud Provider" means Amazon Web Services (AWS), Microsoft Azure (Azure), or Google Cloud Platform (GCP), as selected by Customer.

1.2. "Customer Data" means any data you or your end users upload into USI Atlas.

1.3. "Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data.

1.4. "Information Security Program" means USI’s written security program, policies, and procedures that set forth the administrative, technical, and physical safeguards designed to protect Customer Data.

1.5. "USI Atlas Cluster" means each replica set or sharded cluster of data-bearing nodes running the USI database software that is managed by USI Atlas, subject to your selected configurations.

1.6. "USI Atlas Project" means one or more associated USI Atlas Clusters with a shared set of authorization and network configurations.

1.7. "USI Systems" means USI’s internal infrastructure, including development, testing, and production environments, for USI Atlas.

1.8. "Privileged User" means a select USI employee or third-party contractor who has been granted unique authority to access Customer Data or USI Systems as required to perform their job function.

1.9. "Security Incident Response Plan" means USI’s documented protocols for evaluating suspected security threats and responding to confirmed Data Breaches and other security incidents.

2. Information Security Program Overview.

2.1. General. USI maintains a comprehensive written Information Security Program to establish effective administrative, technical, and physical safeguards for Customer Data, and to identify, detect, protect against, respond to, and recover from security incidents. USI's Information Security Program complies with applicable Data Protection Law and is aligned with the NIST Cyber Security Framework (NIST). Additionally, USI Atlas is certified against ISO 27001:2013, ISO 27017:2015, ISO 27018:2019, SOC 2 Type II, Payment Card Industry Data Security Standard v.4, and Cloud Security Alliance (CSA) Security, Trust, Assurance, and Risk (STAR) Level 2. USI Atlas has also undergone a HIPAA examination validated by a qualified third-party assessor and can be configured to build HIPAA compliant applications.

2.2. Maintenance and Compliance. USI's Information Security Program is maintained by a dedicated security team, led by our Chief Information Security Officer. USI monitors compliance with its Information Security Program, and conducts ongoing education and training of personnel to ensure compliance. The Information Security Program is reviewed and updated at least annually to reflect changes to our organization, business practices, technology, services, and applicable laws and regulations. We will not alter or modify the Information Security Program in a way that materially weakens or compromises the effectiveness of its security controls.

2.3. USI Personnel Controls.

2.3.1. Background Checks. USI performs industry standard background checks on all USI employees as well as any third-party contractor with access to Customer Data or USI Systems.

2.3.2. Personnel Obligations. Any Privileged User authorized to access Customer Data is required to commit in writing to information security and confidentiality obligations that survive termination and change of employment. USI maintains a formal disciplinary procedure for violations by USI personnel of its security policies and procedures.

2.3.3. Training. Upon hire and subsequently at least once per year, Privileged Users authorized to access Customer Data undergo required training on specific security topics, including phishing, secure coding, insider threats, and the secure handling of Customer Data and personally identifiable information. Further, USI implements mandatory, role-specific training for Privileged Users who are authorized to access Customer Data. USI maintains records of training occurrence and content. In addition to these mandatory trainings, USI offers employees additional training resources, such as internal security awareness and education groups and hackathons.

2.4. Third Parties. USI maintains and adheres to a documented process for the evaluation and approval of third-party service providers prior to onboarding, which includes appropriate due diligence regarding each third party's security processes and controls. We require third parties to contractually commit to confidentiality, security responsibilities, security controls, and data reporting obligations, and we perform ongoing targeted due diligence on a quarterly basis.

2.5. Security Contact. If you have security concerns or questions, you may contact us via your normal Support channels, via support.USI.com, or by emailing security@USI.com.

3. USI Atlas Security Controls.

3.1. Data Centers and Physical Storage. USI Atlas runs on AWS, Azure, and GCP, and you control which Cloud Provider to use for deploying your USI Atlas Clusters. Each Cloud Provider is responsible for the security of its data centers, which are compliant with a number of physical security and information security standards detailed at the Cloud Provider's respective websites:

- https://aws.amazon.com/security/
- https://www.microsoft.com/en-us/trustcenter/security/azure-security
- https://cloud.google.com/security/

At least twice per year, each of our Cloud Providers is subject to due diligence performed by USI or third-party auditors, which includes obtaining and reviewing security compliance certifications.

In addition to selecting which Cloud Provider to use, you also control the region where your USI Atlas Clusters are deployed. This gives you the flexibility to decide where your Customer Data is physically stored, and you may choose to deploy your Customer Data in a specific geographic region (for example, only within the European Union or only within the United States).

3.2. Encryption.

3.2.1. Encryption in Transit. All USI Atlas network traffic is protected by Transport Layer Security (TLS), which is enabled by default and cannot be disabled. Customer Data that you transmit to USI Atlas, as well as Customer Data transmitted between nodes of your USI Atlas Cluster, is encrypted in transit using TLS. You can select which TLS version to use for your USI Atlas Clusters, with TLS 1.2 being the recommended default and a minimum key length of 128 bits.

3.2.1.1. Key Management Procedures for Encryption in Transit. All encryption in transit is supported by the use of OpenSSL FIPS Object Module. We maintain documented cryptography and key management guidelines for the secure transmission of Customer Data, and we configure our TLS encryption key protocols and parameters accordingly. USI's key management procedures include: (i) generation of keys with approved key length; (ii) secure distribution, activation and storage, recovery and replacement, and update of keys; (iii) recovery of keys that are lost, corrupted, or expired; (iv) backup/archive of keys; (v) maintenance of key history; (vi) allocation of defined key activation and deactivation dates; (vii) restriction of key access to authorized individuals; and (viii) compliance with legal and regulatory requirements. When a key is compromised, it is revoked, retired, and replaced to prevent further use (except for limited use of that compromised key to remove or verify protections). Keys are protected in storage by encryption and are stored separately from encrypted data. TLS certificates are obtained from a major, widely trusted third-party public certificate authority. In the course of standard TLS key negotiation for active sessions, ephemeral session keys are generated which are never persisted to disk, as per the design of the TLS protocol.

3.2.2. Encryption at Rest. Upon creation of a USI Atlas Cluster, by default, Customer Data is encrypted at rest using AES-256 to secure all volume (disk) data. That process is automated by the transparent disk encryption of your selected Cloud Provider, and the Cloud Provider fully manages the encryption keys. You may also choose to enable database-level encryption via the WiredTiger Encrypted Storage Engine (using AES-256), as well as to bring your own encryption key with AWS Key Management Service (KMS), GCP KMS, or Azure Key Vault (KV).

3.2.3. Encryption in Use. USI Atlas also supports automatic encryption of individual data fields of Customer Data before they are sent to USI Atlas. If you enable this client-side field level encryption feature for a selected data field, an application-side component built into the USI drivers encrypts that field of Customer Data before leaving the driver to be sent to USI Atlas, and only decrypts it upon return to the application once inside the driver. With respect to the Customer Data for which you enable client-side field level encryption, USI Atlas never sees your unencrypted Customer Data and you control the encryption keys, which you can secure using any KMIP-compliant key management service.

3.3. Network Connectivity Options.

3.3.1. Network Isolation. You may choose to deploy your USI Atlas Clusters in a dedicated virtual environment or a shared multi-tenant system. Dedicated USI Atlas Clusters are deployed in a VPC (for AWS and GCP) or VNet (for Azure) that fully isolates your Customer Data and is configured to prevent inbound network access from the internet. Each such USI Atlas VPC or VNet utilizes security groups that act as a virtual firewall for your dedicated USI Atlas Clusters.

3.3.2. Atlas IP Access List. In order to allow inbound network access to your USI Atlas VPC or VNet, you must configure an Atlas IP Access List to enable specific networks to connect to the USI Atlas Clusters within your USI Atlas Project. Unless the Atlas IP Access List for a USI Atlas Project includes a specific network's IP addresses, network traffic is prevented from accessing your USI Atlas Clusters in that USI Atlas Project.

3.3.3. Virtual Private Cloud Peering. You may enable peering between your USI Atlas VPC or VNet to your own dedicated application tier virtual private network with the Cloud Provider of your choice (VPC or VNet). Peering permits you to route encrypted traffic between your USI Atlas VPC or VNet and your own application tier VPC or VNet privately, rather than traversing the public internet. Subject to the capabilities of your selected Cloud Provider, you may also choose to peer your USI Atlas VPC or VNet to your application tier VPC or VNet across regions.

3.3.4. Private Endpoints. USI Atlas also supports private endpoints on AWS using the AWS PrivateLink feature and on Azure using the Azure Private Link feature. If you enable this feature for any USI Atlas Cluster, that USI Atlas Cluster will only allow a one-way connection from your AWS VPC or Azure VNet to the USI Atlas Cluster and that USI Atlas Cluster cannot initiate connections back to your AWS VPC or Azure VNet. Private endpoints also enable you to reach your USI Atlas Cluster transitively over the network from other application tier AWS VPCs and Azure VNets that you have peered with the private endpoint, or through your own self-managed virtual private network including via AWS DirectConnect and Azure ExpressRoute.

3.4. Configuration Management. The USI Atlas environment, including our production environment and your USI Atlas Clusters, leverages configuration management systems to fully automate configuration based on one-time decisions that are securely applied to new and existing environments to ensure consistency every time. Our production environment and your USI Atlas Clusters use in-house built machine images with secure configuration management applied via industry standard automation software, which includes hardening steps.

4. Access Controls.

4.1. Customer Access. USI Atlas supports multiple authentication and authorization options and methods to give you the flexibility to meet your individualized requirements and needs. You are responsible for understanding the security configuration options available to you and the impact of your selected configurations on your USI Atlas environment, which consists of a web application administrative interface (“USI Atlas UI”) and any USI Atlas Cluster you deploy. USI Atlas provides you with configurable authentication and authorization options for both the USI Atlas UI and your USI Atlas Clusters.

4.1.1. USI Atlas UI Authentication and Authorization. User credentials for the USI Atlas UI are stored using industry standard and audited one-way hashes. The USI Atlas UI supports multi-factor authentication (MFA), including a security key/biometrics option that enables you to use hardware security keys or built-in authenticators. The USI Atlas UI also supports federated authentication functionality for Single Sign-On (SSO) utilizing Security Assertion Markup Language (SAML).

4.1.2. USI Atlas Cluster Authentication and Authorization. Authentication control for a USI Atlas Cluster is enabled by default with the Salted Challenge Response Authentication Mechanism (SCRAM). You may choose to manage user authentication with self-managed X.509 certificates or through AWS IAM Users or Roles. USI Atlas allows you to define permissions for individual users or applications in order to restrict the Customer Data that is accessible in a query. Further, you may choose to assign each user a USI Atlas Project-specific role, which authorizes that user to perform specific actions on the USI Atlas Clusters within that USI Atlas Project. The USI Atlas UI allows you to tailor your access controls by combining multiple roles and privileges for particular users. You can review, limit, and revoke user access to your USI Atlas Clusters at any time. USI Atlas also provides you with the ability to manage user authentication and authorization using your own Lightweight Directory Access Protocol (LDAP) server over TLS. A single LDAP over TLS (LDAPS) configuration applies to all USI Atlas Clusters in a USI Atlas Project.

4.1.3. Credential Requirements. As part of the configuration options, you may establish minimum password requirements (e.g., length, complexity) through your identity provider after federating authentication to the USI Atlas UI via SAML and to the USI Atlas Clusters via LDAPS.

4.1.4. Customer Database Auditing. USI Atlas offers granular auditing that monitors actions in your USI Atlas environment and is designed to prevent and detect any unauthorized access to Customer Data, including create, read, update, and delete (CRUD) operations, encryption key management, and role-based access controls. You are responsible for enabling database auditing and selecting the users, roles, groups, and event actions that you want to audit.

4.2. USI Personnel Access to USI Atlas Clusters.

4.2.1. Privileged User Access. As a general matter, USI personnel do not have authorization to access your USI Atlas Clusters. Only a small group of Privileged Users are authorized to access your USI Atlas Clusters in rare cases where required to investigate and restore critical services. USI adheres to the principle of “least privilege” with respect to those Privileged Users, and any access is limited to the minimum time and extent necessary to repair the critical issue. Privileged Users may only access your USI Atlas Clusters via a gated process that uses a bastion host, requires MFA both to log in to our USI Systems and to establish a Secure Shell connection (SSH) via the bastion host, and requires approval by USI senior management.

4.2.2. Restricting USI Personnel Access. USI Atlas provides you with the option to entirely restrict access by all USI personnel, including Privileged Users, to your USI Atlas Clusters. If you choose to restrict such access and USI determines that access is necessary to resolve a particular support issue, USI must first request your permission and you may then decide whether to temporarily restore Privileged User access for up to 24 hours. You can revoke the temporary 24-hour access grant at any time. Enabling this restriction may result in increased time for the response and resolution of support issues and, as a result, may negatively impact the availability of your USI Atlas Clusters. If you enable client-side field level encryption, even Privileged Users will be unable to access Customer Data within your USI Atlas Clusters in the clear unless you provide USI with the encryption keys.

4.2.3. Credential Requirements. Privileged User accounts may only be used for privileged activities, and Privileged Users must use a separate account to perform non-privileged activities. Privileged User accounts may not use shared credentials. The password requirements described in Section 4.3.3 also apply to Privileged User accounts.

4.2.4. Access Review and Auditing. USI reviews Privileged User access authorization on a quarterly basis. Additionally, we revoke a Privileged User’s access when it is no longer needed, including within 24 hours of that Privileged User changing roles or leaving the company. We also log any access by USI personnel to your USI Atlas Clusters. Audit logs are retained for at least six years, and include a timestamp, actor, action, and output. USI utilizes a combination of automated and human review to scan those audit logs.

4.3. USI Personnel Access to USI Systems.

4.3.1. General. USI’s policies and procedures regarding access to USI Systems adhere to the principles of role-based access control (RBAC), least privilege, and separation of duties. In accordance with these principles, with respect to USI Atlas, USI developers are only granted access to our development environments, and access to our production environment is limited to Privileged Users with appropriate authorizations. We review access authorizations to USI Systems on a quarterly basis and we review any changes to authorizations for Privileged Users immediately. As part of the employee off-boarding process, access to USI Systems is revoked within 24 hours of an employee’s departure.

4.3.2. Access to USI Atlas Production Environment. Our backend production environment that runs USI Atlas is only accessible by a dedicated group of Privileged Users whose privileges must be approved by senior management. Privileged Users may only access our backend production environment via a bastion host and doing so requires MFA both to log in and to establish a SSH via the bastion host.

4.3.3. Credential Requirements. All USI personnel passwords must conform to industry-standard complexity rules. Additionally, MFA is mandatory for all USI personnel and cannot be disabled.

4.4. Physical Controls at USI Offices. As noted in Section 3.1, Customer Data is deployed at the data centers of your selected Cloud Provider, and not at facilities owned or operated by USI. At USI offices, we follow industry best practices to employ physical security controls that are appropriate to the level of risk posed by the information stored and the nature of operations at our offices. In our offices, we: (i) issue access cards for all personnel through formal provisioning and approval processes; (ii) limit access to restricted areas to personnel with a need to access those areas to carry out their job functions; (iii) require visitors to sign in, execute a non-disclosure agreement, and be escorted in all non-public spaces; (iv) employ surveillance systems to monitor activity at points of entry from public spaces; and (v) revoke personnel access within 12 hours of termination.

4.5. Secure Deletion of Customer Data. If you terminate a USI Atlas Cluster, it will become unavailable to you immediately and any Cloud Backup associated with that USI Atlas Cluster will be terminated. USI may retain a copy of the Customer Data stored in the terminated USI Atlas Cluster for up to 5 days. If you terminate Cloud Backups, all snapshots will become unavailable to you immediately and it may take up to 24 hours for the Customer Data contained in the snapshots to become unrecoverable. When you terminate a USI Atlas Project, the master key used to encrypt Customer Data is securely wiped, rendering all Customer Data effectively unrecoverable. If you choose to use USI Atlas Online Archive, you can delete the entire archive, or pre-define automatic deletion dates for different data sections within USI Atlas Online Archive to help automate any applicable retention restrictions or policies.

5. USI Systems Security.

5.1. Separation of Production and Non-Production Environments. USI Atlas has strict separation between production and non-production environments. Our USI Atlas production environment, your USI Atlas Clusters, and your Customer Data are never utilized for non-production purposes. Our non-production environments are utilized for development, testing, and staging. USI also maintains firewalls to achieve strict separation of our USI Atlas production environment and USI's internal network.

5.2. Software Development Lifecycle. USI has a dedicated security team, reporting to the Chief Information Security Officer, that leads security initiatives in the software development lifecycle (SDLC). We develop new products and features in a multistage process using industry standard methodologies that include defined security acceptance criteria and align with NIST and OWASP guidance. The SDLC includes regular code reviews, documented policies and procedures for tracking and managing all changes to our code, continuous integration of source code commits, code versioning, static and dynamic code analysis, vulnerability management, threat modeling, and bug hunts, as well as automated and manual source code analysis.

5.3. Monitoring and Alerting. USI monitors the health and performance of USI Atlas without needing to access your USI Atlas Clusters. USI maintains a centralized log management system for the collection, storage, and analysis of log data for our USI Atlas production environment and your USI Atlas Clusters. We use this information for health monitoring, troubleshooting, and security purposes, including intrusion detection. We maintain our log data for at least six years, and we utilize a combination of automated scanning, automated alerting, and human review to monitor the data.

5.4. Vulnerability Management.

5.4.1. USI Atlas Vulnerability Scanning. USI maintains a documented vulnerability enumeration and management program that identifies internet-accessible company assets, scans for known vulnerabilities, evaluates risk, and tracks issue remediation. We conduct quarterly scans of both the underlying systems upon which USI Atlas is deployed, as well as all third-party code integrated into our products. USI's vulnerability management policy requires individual engineering teams to identify known vulnerabilities in system components, and develop remediation timeframes commensurate to the severity of an identified issue. We also utilize automated tooling in conjunction with monitoring security bulletins for relevant software and libraries, and implement patches if security issues are discovered.

5.4.2. Vulnerability Remediation. USI uses a central company-wide ticketing system to track all security issues until remediation. We implement patches to our operating system and applications on a need-to-update basis, as determined in accordance with the Common Vulnerability Scoring System (CVSS). We are also a Mitre CVE Numbering Authority (CNA). Development tasks for all patches, bug fixes, and new features are defined as issues for specific target releases and are deployed to production only after completing requisite checkpoints, including quality assurance testing, staged deployment, and management review.

5.5. Penetration Testing and Internal Risk Assessments. USI Atlas undergoes regular reviews from both internal and external security teams.

5.5.1. External Testing. Our USI Atlas production environment is subject to an external penetration test by a nationally recognized security firm at least once per calendar year. Upon request, we will provide you with a summary letter of engagement that includes the number of high, medium, and low issues identified, but due to the sensitivity of the information gathered during these tests, we cannot allow customers to perform testing of our production platform. Application-level security testing uses a standard application assessment methodology (e.g., OWASP). Additionally, external engagements with security consultants may include social engineering and phishing testing.

5.5.2. Internal Testing. Internally, USI Atlas undergoes periodic risk assessments, including technical vulnerability discovery and analysis of business risks and concerns. The USI security team is also routinely involved in source code review, architecture review, code commit peer review, and threat modeling.

6. Contingency Planning.

6.1. High Availability and Failover. Every USI Atlas Cluster is deployed as a self-healing replica set that provides automatic failover in the event of a failure. Replica set members are automatically provisioned by USI Atlas across multiple availability zones within a region, providing resilience to localized site failures. All replica set members are full data-bearing nodes, ensuring majority writes in the event of single node failure and higher resilience during recovery. Concurrent writes across replica sets occur in real time. USI Atlas also offers multi-region and multi-cloud deployment options.

6.2. Backups. USI Atlas offers Cloud Backups, which use the native snapshot functionality of your selected Cloud Provider to locally back up your Customer Data. You may enable Cloud Backups when you create or modify a USI Atlas Cluster, and you have control over how often a Cloud Backup is captured and the length of time for which Cloud Backups are retained. Cloud Backup snapshots are stored with your selected Cloud Provider in the primary region of your USI Atlas

Cluster. All Cloud Backups are encrypted at rest and you may choose to use self-managed keys with the WiredTiger Encrypted Storage Engine. You may also optionally enable Continuous Cloud Backups with point-in-time recovery stored on our encrypted S3 buckets.

6.3. Business Continuity and Disaster Recovery. USI maintains a documented business continuity and disaster recovery ("BCDR") plan that aligns with ISO/IEC 22301:2019. Our BCDR plan includes: (i) clearly defined roles and responsibilities; (ii) availability requirements for customer services, including recovery point objectives (RPOs) and recovery time objectives (RTOs); and (iii) backup and restoration procedures. We review, update, and test our BCDR plan at least annually. In the event of an incident that triggers the BCDR plan, the RPO will depend on your impacted USI Atlas Cluster and backup configurations. You can test how your application handles a replica set failover at any time using the USI Atlas UI or API.

7. Incident Response and Communications.

7.1. Security Incident Response Plan. As part of the Information Security Program, USI maintains an established Security Incident Response Plan that aligns with NIST and ISO/IEC 27001:2013. In the event that USI becomes aware of a Data Breach or other security incident, USI will follow the Security Incident Response Plan, which includes: (i) clearly defined roles and responsibilities, including designation of a security incident task force; (ii) reporting mechanisms; (iii) procedures for assessing, classifying, containing, eradicating, and recovering from security incidents; (iv) procedures and timeframes for required notifications to relevant authorities and customers; (v) procedures for forensic investigation and preservation of event and system log data; and (vi) a process for post-incident and resolution analysis designed to prevent future similar incidents. The Security Incident Response Plan is reviewed, updated, and tested annually, including a security tabletop exercise at least once per year.

7.2. Security Incident Tracking. USI maintains a comprehensive security incident tracking system that aligns with ISO/IEC 27001:2013 and documents: (i) incident type and suspected cause; (ii) whether there has been unauthorized or unlawful access, disclosure, loss, alteration, or destruction of data; (iii) if so, the categories of data affected by the incident, including categories of personal information; (iv) the time when the incident occurred or is suspected to have occurred; and (v) the remediation actions taken.

7.3. Customer Communications. USI will notify you without undue delay if we become aware of any Data Breach. Taking into account the information available to us, such notice will include a description of the nature and cause of the Data Breach and the expected resolution time. To the extent possible, we will subsequently update you with information regarding evaluation of the root cause, potential impact, remediation actions taken, and actions planned to prevent a future similar event.

8. Audit Reporting.

8.1. Third-Party Certifications and Audit Reports. Upon request, and subject to the confidentiality obligations set forth in the Agreement, we will make available to you (or your independent, third-party auditor) information regarding USI's compliance with the security obligations set forth in these Security Measures in the form of third-party certifications and audit reports.

8.2. Security Questionnaires. No more than once per year, we will complete a written security questionnaire provided by you regarding the controls outlined in these Security Measures.

USI Security Guide to MongoDB Atlas

MongoDB Atlas is a database as a service created by the experts who design and engineer MongoDB. With MongoDB Atlas, MongoDB, Inc. helps customers manage database operations and the underlying infrastructure.

There are 3 key components that make up MongoDB Atlas:

- *Automation* orchestrates provisioning, database deployment, configuration, and lifecycle management for MongoDB on instances hosted in the public cloud (AWS).

- *Monitoring* collects and displays key database and underlying hardware metrics. Customized alerting is included as part of MongoDB Atlas monitoring.

- *Backup* provides a fully managed continuous backup service with point-in-time recovery. Backup is an add-on service priced at $2.50/GB/mo.

As with all software, administrators must consider security and risk exposure for a MongoDB Atlas deployment. A Defense in Depth approach that addresses a number of different methods for managing risk and reducing risk exposure is recommended for securing MongoDB Atlas deployments. There are no magic solutions for risk mitigation, and maintaining a secure deployment is an ongoing process.

MongoDB Atlas features extensive capabilities to defend, detect, and control access to MongoDB, including:

- User Credentials
- Database Authentication, Authorization, and User Rights Management
- Network Isolation
- IP Address Whitelisting
- AWS VPC Peering
- Encryption for data-in-transit
- Encryption for data-at-rest
- High Availability
- Encrypted Backups
- Change Management

MongoDB, Inc. also maintains organizational security practices and policies, including:

- Security Program
- MongoDB, Inc. Access
- Application Security Review
- Communication and Notifications Practices

User Credentials

User credentials for MongoDB Atlas are stored using industry-standard and audited one-way hashing mechanisms. Customer sensitive data provided within the GUI, such as passwords, keys, and credentials which must be used as part of the service are stored encrypted. In order to ensure data is protected and restricted, customer data is segregated via logical controls.

Network Isolation

MongoDB Atlas customers' data and underlying systems are fully isolated from other customers. Each customer group is contained in its own Amazon Virtual Private Cloud (VPC)[1] and dedicated firewall (security group). All database clusters associated with a group are deployed inside the associated VPC. MongoDB Atlas instances are provisioned for customers when they create a cluster; each *mongod* process is deployed to its own AWS EC2 instance.

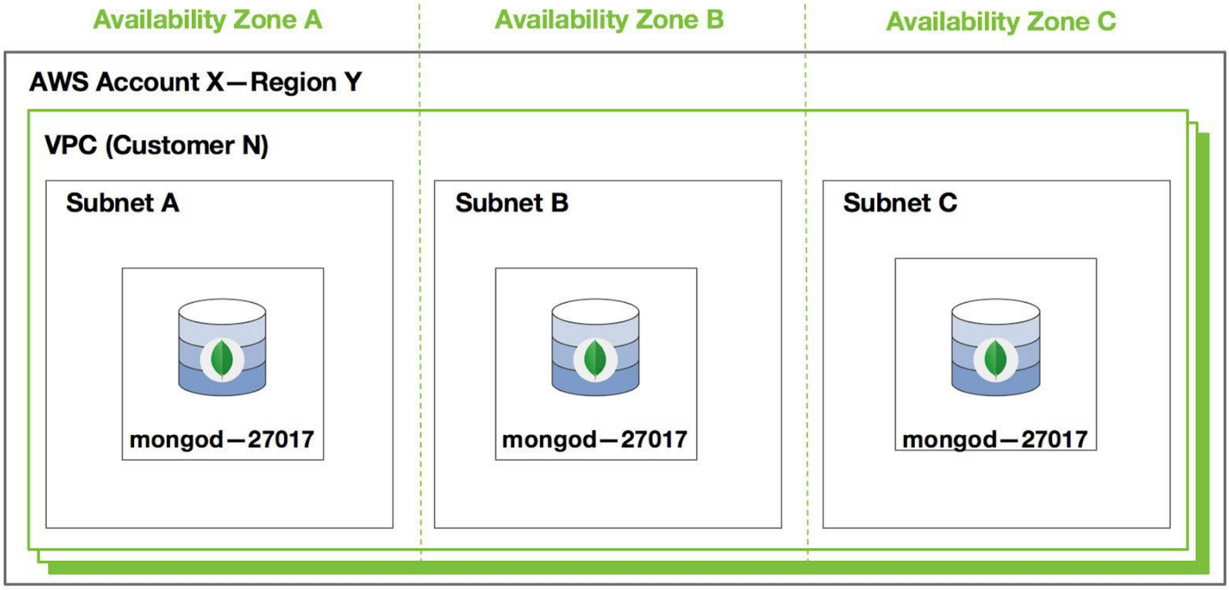


Figure 1: The above graphic represents MongoDB Atlas's isolation and dedicated assets. The Virtual Private Cloud (VPC) and all assets within each subnet are unique and dedicated per customer and are not shared between customers.

[1] https://aws.amazon.com/vpc/

Database Authentication, Authorization, and User Rights Management

With MongoDB Atlas, authentication is automatically enabled by default via the SCRAM-SHA-1 authentication mechanism to help ensure a secure system out of the box.

MongoDB Atlas allows administrators to define permissions for a user or application, and what data can be accessed when querying MongoDB. MongoDB Atlas provides the ability to provision users with roles specific to a group or database, making it possible to realize a separation of duties between different entities accessing and managing the data.

IP Address Whitelisting

Application servers are prevented from accessing the database unless their IP addresses (or a CIDR covering their IP addresses) have been added to the IP whitelist for the appropriate MongoDB Atlas group.

As a default security standard, MongoDB Atlas requires all groups to define an IP Whitelist, however if users actively do not wish to restrict access through this route, they can simply provide a open CIDR (0.0.0.0/0).

AWS VPC Peering

MongoDB Atlas customers can use AWS VPC Peering, which allows users to create an extended, private network that connects the AWS VPC housing their application servers with the VPC containing their backend MongoDB Atlas databases. VPC peering achieves this connectivity without using public IP addresses, and without the need to whitelist every client in a MongoDB Atlas group. This feature requires that the two connecting VPCs are located in the same AWS region.

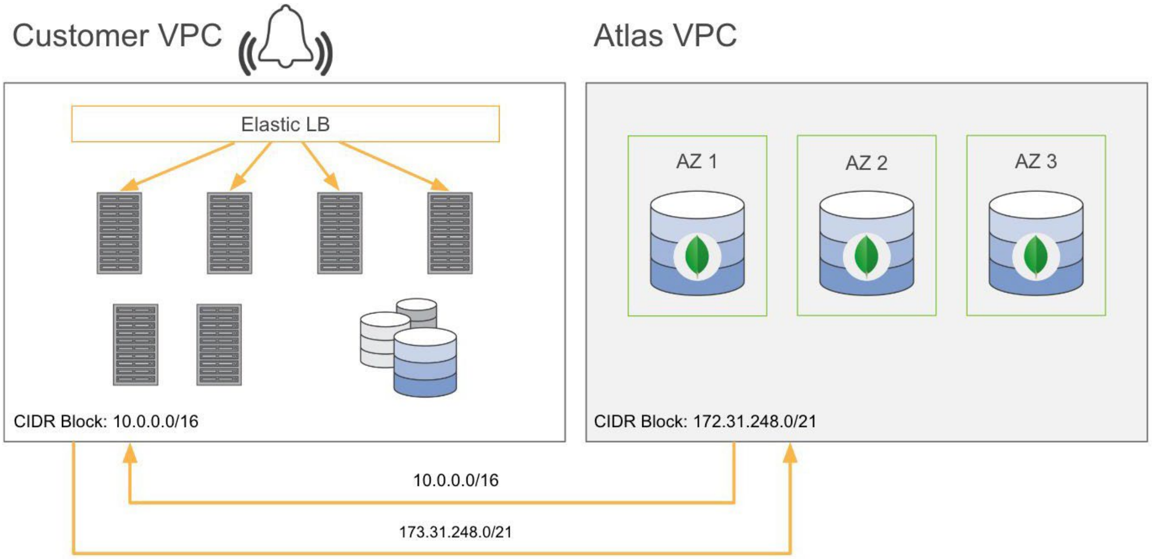
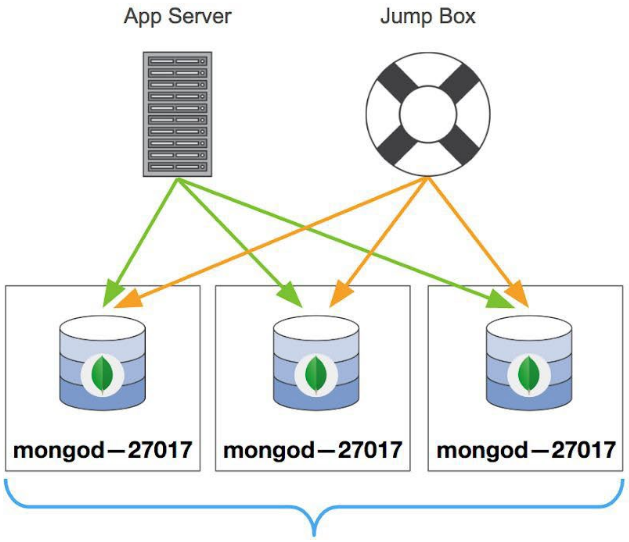


Figure 2: The above graphic shows a MongoDB Atlas VPC peered to an AWS VPC containing a customer's application servers. Note that users cannot create a VPC peering connection between VPCs with matching or overlapping CIDR blocks.

Encryption

All MongoDB Atlas users have several key MongoDB Security features enabled by default; SSL/TLS and authentication is enabled by default and cannot be disabled. Traffic from any client or entity capable of connecting to MongoDB Atlas is authenticated and encrypted in-transit, and traffic between customer's internally managed MongoDB nodes is also authenticated and encrypted in-transit. MongoDB Inc. follows best practices as it pertains to SSL/TLS security and updates SSL/TLS configurations to adjust offered ciphers/algorithms in order to account for current security best practices.



One security group per VPC applied to all Amazon EC2 instances

Three classes of security rules:

- MongoDB traffic between cluster members
- MongoDB traffic between application and clusters
- SSH traffic between production support jump box and EC2 instance

At-rest encryption is available to Atlas customers with Amazon EBS encryption. Users can select this option, which uses industry standard AES-256 encryption to secure all volume (disk) data, when provisioning their instances.

High Availability & Failover

With regard to service availability, every MongoDB Atlas cluster is deployed as a self-healing replica set which provides automatic failover in the event of a failure. Replica set members are automatically provisioned by MongoDB Atlas across multiple availability zones within a region, providing resilience to localized site failures. All replica set members are full data bearing nodes, ensuring majority writes in the event of single node failure and higher resilience during recovery.

MongoDB Atlas does not currently support *cross-region* deployments at this time. As an example, a single MongoDB Atlas cluster with 3 replica sets in the us-east-1 region will consist of MongoDB replicating across three distinct AWS data-centers within the same geographical region. For more information, please see AWS's regions and availability zones[2] documentation.

[2] http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html

Backup

Enabling backup for your MongoDB Atlas cluster allows you to restore or archive from stored snapshots or from a point in time between snapshots.

For MongoDB Atlas clusters in AWS eu-west-1 where backups were initiated after January 31, 2017.

Backup snapshots are stored on AWS encrypted EBS volumes and encrypted S3 storage in-region.

For all other MongoDB Atlas clusters

Backup snapshots are stored in MongoDB co-located facilities in the US Northeast. All data centers are monitored 24x7 and are SSAE-16 compliant. For high availability, the data centers run active/active. Data center controls include redundant power and environmental controls, dedicated equipment enclosures, 24x365 staffed building security, multi-factor physical access controls, CCTV, and more. Data centers are physically and logically separate from MongoDB offices; physical access is restricted to MongoDB operational personnel only.

MongoDB Atlas provides optional encrypted backup for prepay customers with an annual contract. With this option, a customer's backup data is stored encrypted-at-rest using Seagate Self-Encrypting-Drive (SED) Technology:

- Enterprise-Class SED drivers perform full-disk encryption at the hardware level
- Encryption is performed via an encryption engine built into drive hardware, using the standard AES-256 encryption algorithm operating in CBC mode
- The SED ensures all data is encrypted prior to being written to physical media and decrypted as it is read from the media.
- The encryption engines are always in operation and cannot be disabled

Patch Management

Patching of operating system and applications are performed on a need-to-update basis. MongoDB, Inc. employees monitor security bulletins for relevant software and implement patches if critical issues are discovered. The MongoDB server software itself is continuously updated as new versions are released.

With respect to change management, development tasks are defined as issues for specific target releases. A release is deployed to production after it has transitioned through the requisite checkpoints, including testing, staged deployment, and management review. All internal release notes include a QA test plan.

Security Program

MongoDB internal security practices and policies are aligned to be compliant with ISO 27002 controls. MongoDB's Security Program is lead by a dedicated security team.

MongoDB employees are provided with periodic security training and a company security handbook which describes security procedures and required practices, such as data sensitivity and handling, security reporting and systems security.

MongoDB has a vulnerability enumeration and management program; this program identifies company assets, scans for known vulnerabilities, evaluates risk and tracks issue remediation. Vulnerability scans occur at least daily, with results reporting to a centralized security dashboard. A central company-wide ticketing system is used to track all security issues until remediation. Application level security testing using a standard application assessment methodology (e.g., OWASP) is also performed periodically by both internal teams and external consultants. Systems are patched as needed. Security-related patches are applied commensurate to their severity.

Human Resources performs multi-residence criminal background checks on all prospective employees. The HR employee off-boarding processes includes verification of account access termination.

MongoDB, Inc. Access

Technical role-based access controls are in place to ensure only MongoDB employees with approved operational roles can access MongoDB Atlas back-end systems. Access to sensitive systems and actions requires multi-factor authentication. Employee access is controlled via role-based access control methods, and permissions are regularly audited.

Operational access to underlying hosts requires the use of multi-factor authentication and utilization of a bastion host. Access to underlying hosts is restricted solely to MongoDB operational personnel who have been granted express access by senior management and have a work need to access systems.

MongoDB maintains a centralized log management system for collection, storage and analysis of log data for production environments. This information is used for health monitoring, troubleshooting and security purposes.

Application Security Review

MongoDB Atlas has undergone review by our internal Security Team as well as external third party consultants. Any identified security issues are tracked in our internal ticketing system and resolution is integrated into the existing development life cycle.

We engage external security assessment forms to perform application security testing of MongoDB Atlas. A copy of the most recent letter of engagement, which includes timeframe, scope and description of what was tested, is available for customers to review, upon request.

Communications and Notifications

It is the expectation of MongoDB that customers do not send us data which would be prohibited by legal or other regulatory framework. In the event that a customer sends us sensitive data in error, we ask to be informed immediately so we can take appropriate action, which may include data destruction.

MongoDB has an established Incident Response and Critical Communications Policy. In the event that a security alert/event, or other signal results in MongoDB declaring a security incident, MongoDB will follow its internal incident response protocols and inform affected customers as soon as practicable.

Additional Resources

MongoDB Security Alerts and Contact
https://www.mongodb.com/security

MongoDB Security Checklist
https://docs.mongodb.org/manual/administration/security-checklist

MongoDB Atlas Best Practices White Paper
https://www.mongodb.com/collateral/mongodb-atlas-best-practices

MongoDB Atlas FAQ
https://www.mongodb.com/cloud/atlas/faq

MongoDB Atlas Implementation Details
http://experience.mongodb.com/spotlight/mongodb-atlas-implementation-deep-dive-506482

Privacy Policy
https://www.mongodb.com/legal/privacy-policy