Couchbase

WHITEPAPER

Couchbase Capella™ Security and Data Protection

Contents

ABOUT COUCHBASE

Couchbase provides a leading modern NoSQL database that empowers enterprises to build, manage, and operate modern mission-critical applications that demand high performance at scale. Couchbase's database is versatile and works in multiple configurations, from cloud to multicloud or hybrid cloud, to on-premise environments to the edge, and can be managed by Couchbase or the customer Organization. For Organizations wanting a fully managed database solution, Couchbase delivers Couchbase Capella™, a Database-as-a-Service (DBaaS) offering that leading enterprises across the globe can trust to run their business-critical applications or services.

Our culture starts with Couchbase values, and the people are its champions. Couchbase's values are:

Be Valued	Create Value
Be a Good Human, *Always*.	Attack Hard Problems, *Driven by Customer Outcomes*.
Act With Uncompromising Integrity, *Period*.	Play to Win, *Together*.
Serve Your Family, *As Defined By You*.	Make Tomorrow Better Than Today, *Start Now*.

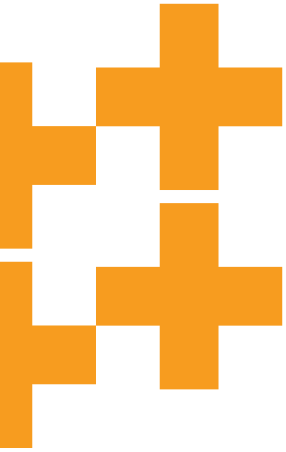
SECURITY AT COUCHBASE

At Couchbase, we understand that the security of our products and cloud offerings are important to Organizations. Couchbase management demonstrates a commitment to security by setting forth policies, establishing strategic direction, providing resources, and empowering employees. Industry best practices and security by design are ingrained in the policies, procedures, software development practices, and cloud security.

A dedicated Information Security (Infosec) group is responsible for governance, risks, and compliance management and maintaining the information security management system (ISMS) at Couchbase. Security is also a responsibility that is shared and supported by all employees. The board of directors leverages their expertise to provide independent oversight of the development of relevant controls. An audit committee monitors the effectiveness and performance of internal security controls through key performance indicators (KPIs) and key risk indicators (KRIs).

Engineering teams are responsible for developing a secure product by following a secure software development life cycle (SDLC). Couchbase Capella cloud team is responsible for deploying and maintaining security for production environments. Operational security is the responsibility of all business units as applicable.

HIRING, SECURITY, AWARENESS, AND TRAINING



Security at Couchbase starts with strong hiring practices. Background screening is performed for all employees and as a condition of employment, employees are required to sign confidentiality and non-disclosure agreements. Couchbase maintains an employee handbook that contains organizational policy statements, behavioral standards, codes of conduct, and disciplinary policies to which employees are required to comply.

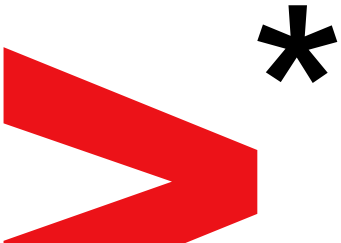
All Couchbase employees are assigned security and privacy training; security training must be completed within a defined schedule upon hire and annually thereafter. In addition, role-specific training is available for engineering teams that focus on cloud security, secure design, and Open Web Application Security Project (OWASP) top 10 risks. Additionally, the Infosec team periodically conducts simulated phishing attacks to reinforce cybersecurity awareness and communicates security best practices to all personnel.

GOVERNANCE, RISK, AND COMPLIANCE

The Infosec team at Couchbase maintains information security policies, risk management processes, and compliance with regulatory and industry standards relevant to information security. The Infosec team also conducts annual risk assessments in collaboration with Couchbase's technical and business units. The identified risks are recorded and monitored. In addition, the Infosec team tracks the implementation of the risk-mitigating controls to ensure the protection of Organizations and business assets and compliance with contractual and regulatory obligations.

CORPORATE OPERATIONAL SECURITY

Couchbase has established operational requirements that support the achievement of service commitments to its customers, relevant laws and regulations, and system requirements related to security, availability, and confidentiality.



Data classification and retention

Couchbase has defined a data classification scheme that mandates a specific level of protection for each data type. In addition, data retention controls are enforced to comply with legal requirements.

Baselines and secure defaults

Technical teams maintain baseline configuration standards for all operating systems (OS). New instances are spawned from standard baselined images that are hardened for security. Baseline configurations are generally derived from industry-standard benchmarks, including vendors' security best practices and changing or removing default parameters.

Incident management

Couchbase has an approved Incident Management policy and a well-defined process to detect, respond, contain, analyze, recover, and repair security incidents throughout the incident life cycle. The Infosec team leads the process, facilitates security incident management activities, and provides relevant and impacted groups with guidance. In addition, the security incident response team (SIRT) meets periodically and performs incident management tabletop exercises to improve the process.

Vendor risk management

The Infosec team enforces an onboarding process on all new vendors to collect and document their use and conduct a vendor risk assessment to review their security posture and compliance with Couchbase information security requirements. Vendors and service providers are classified based on their risk profiles and potential impact on Couchbase and its customers.

Vulnerability management

The vulnerability management program covers infrastructure, systems, Couchbase Server, and Couchbase Capella. The Infosec team manages the quarterly vulnerability scans using internal and external scanners. Vulnerabilities discovered are classified according to their severity, tracked, and mitigated promptly.

Endpoint security

The corporate IT team installs and centrally manages antivirus software on all Couchbase-issued laptops to protect against malware and spyware. End users are not allowed to alter or disable the antivirus software. Endpoint devices are regularly updated with the latest OS and software patches as they are released and recommended by the vendor. Couchbase-owned laptops and workstations used to store or access non-public data have full-disk encryption enabled.

CORPORATE NETWORKS PROTECTION

Firewalls are deployed at Couchbase corporate and cloud networks' entry points to prevent unauthorized access. In addition, intrusion detection, prevention, and distributed denial of service attack (DDoS) protection mechanisms are implemented to monitor and safeguard Couchbase systems and networks. Firewalls and network configurations are periodically reviewed to ensure compliance with baseline configurations.

CORPORATE PHYSICAL SECURITY

Couchbase corporate office building doors are locked and require a badge or key fob issued by the workplace team. Entry to sensitive or high-risk areas is restricted to authorized personnel only. Visitors to Couchbase offices are required to register and are accompanied by an employee. The locks are changed when a key is lost, or combinations are compromised for organization-defined high-risk entry/exit points.

BUSINESS CONTINUITY AND DISASTER RECOVERY

Business continuity and disaster recovery plans are developed, updated, and tested annually. Additionally, backup restoration tests are also performed annually. Business continuity and disaster recovery plans are updated and reviewed on an annual basis. Any updates to business continuity and disaster recovery plan are made after testing is complete.

COUCHBASE CAPELLA SECURITY

Capella is a fully managed Database-as-a-Service (DBaaS) that eliminates your database management efforts and reduces operational costs. Couchbase understands the significance that Organizations place on security in the cloud and has hence implemented robust technical and security safeguards to protect cloud assets and Organizations' data. Here is how Couchbase Capella keeps Organizations' data safe.

The Couchbase Capella architecture is based on industry best practices for security and rests on three important pillars: Verify Explicitly, Least Privilege, and Platform Monitoring.

VERIFY EXPLICITLY

Verify Explicitly calls for strong identity authentication and explicit verification of access to data. This is accomplished using role-based access controls (RBAC) to

ensure only authorized Users or Organizations' applications with the authorized database credentials have access to the data. Further, all users, machine-to-machine, and machine-to-user access is enforced by authentication and authorization.

LEAST PRIVILEGE

Enforcement of Least Privilege access is applied to all credentials and secrets thus ensuring strict access controls to sensitive data and actions. Multi-factor authentication is available to verify users and actions performed on the system. Role-based access control associates users with specifically assigned privileges to provide only the least amount of access required to fulfill the role. Upon authentication, user roles are determined. If they allow the form of system access the user is attempting, then access is granted. Otherwise, it is denied.

PLATFORM MONITORING

To prevent potential breaches, Capella implements a managed cloud intrusion detection system that involves 24x7 monitoring to detect unauthorized access, identity and access management (IAM) updates, and monitoring of security configurations.

Capella solution architecture

Capella's high-level architecture consists of Organizations, Projects, Clusters, Buckets, and Users with the right access control for these resources.

- **Organization** is the top-level artifact and everything a customer does in Couchbase Capella – whether it's creating a cluster or managing billing – happens within the extent of an organization. To be a member of an Organization, a Couchbase Capella user account is required. If the client accepts an invitation from an Organization to create an account, that client joins that Organization.
- **Projects** are a logical container for Clusters. There can be multiple Projects in an Organization. Projects are a convenient way to logically group workloads and isolate them from each other, separate production and development environments, or group clusters by application.
- **Users** added to an Organization are assigned one or more Organizational roles which control the privileges those users have within the Organization. They determine the privileges users have within the scope of the Project and they determine whether a Project member can do things like create database credentials, create and manage Clusters in the Project, or only view and monitor Clusters.
- **Clusters** are managed deployments of the Couchbase Server. A Cluster consists of one or more instances of Couchbase Server, each running on an independent node.
- **Buckets** are the containers for data; these are the equivalent to databases and data inside a bucket is organized into groups of scopes (similar to RDBMS schemas), which contain groups of collections (similar to RDBMS tables).

Capella is designed with two major components. The Control Plane is the user interface for management and the Data Plane houses the Couchbase database.

CONTROL PLANE

The Control Plane is an interface available to Organizations for managing the end-to-end life cycle of data planes. The Control Plane hosts all the necessary services and run jobs which enables the life cycle management of data plane services that are deployed in the chosen cloud service provider.

DATA PLANE

The Data Plane is the combination of the server database, storage, infrastructure components, and database management aspects. To ensure the separation of an Organization's data, each Organization is assigned a unique account within a chosen cloud provider. The Data Plane is encompassed within a VPC in that account.

CENTRALIZED MANAGEMENT

The Capella Control Plane decouples the control and data for isolation of an Organization's data. The Control Plane also isolates secrets stored for the control of data in the Data Plane. Role-based access control, identity and access management, and database users are all managed via the Control Plane.

ACCESS FROM THE CONTROL PLANE

The Control Plane has restricted access to the Data Plane to perform specific functions such as gathering logs or triaging the environment. It performs these functions using temporary credentials using secrets. This is done without human interaction to isolate the data in a bucket from the Control Plane. The Control Plane application uses only the base status IAM access key and secret key to assume a role or get temporary credentials to perform a task. These underlying base credentials expire after a set period of time. Any access of the database RBAC permissions and direct queries in the Data Plane would require access to the secrets which would trigger an alert to the Couchbase Capella Operations Team.

SECURE DEVELOPMENT LIFE CYCLE

Couchbase Capella was developed with modern DBaaS principles in mind. Secure development practices as well as secure repositories are utilized to protect the Organization's intellectual property. Build and image integrity ensures that all code running in Capella is secured. Standardized code review practices are enforced during each iteration. Vulnerability scanning is in use, as well as best practices for the life cycle of trusted images used in the deployment of Couchbase Capella. Security scanning is done periodically on the code. Containers must be signed before they can be run which prevents any unvalidated code. Additionally, software scans are performed on the Control Plane virtual machines (VMs), container images, and serverless functions.

Capella compliance

Couchbase employs a defense-in-depth security approach to secure Organizations' data as well as Couchbase assets, data, and services. This model ensures that a failure at one control layer should not affect the entire organization or result in a large-scale breach. The Infosec team has established a security program based on Couchbase's identified risks, industry standards, and best practices (which include,

but are not limited to, CIS Critical Security Controls, ISO 27002, NIST SP 800-53, SSAE 18 SOC 2 Trust principles) as applicable. In addition, independent third-party consultants audit the security program annually. As a result, the Infosec program is continuously reviewed and iteratively improved.

CAPELLA SSAE 18 SOC 2 COMPLIANCE

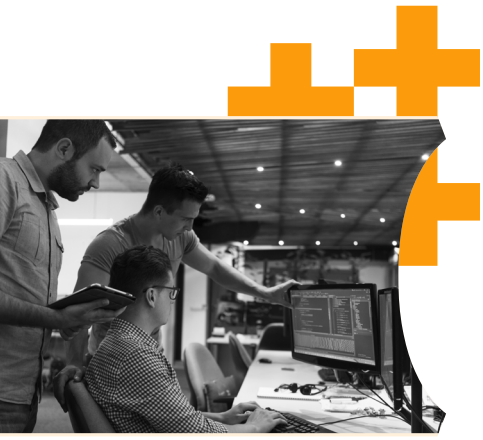
Capella has completed a SOC 2, Type II audit and received a report that shows Couchbase has designed and implemented controls based on the SOC 2 Trust Services Criteria to provide reasonable assurance of Couchbase's service commitments.

HIPAA COMPLIANCE

Capella offers security and privacy controls, which have been audited by an external audit process, designed to address the requirements of HIPAA to allow organizations to store and manage protected health information (PHI) in Capella. Organizations that qualify as covered entities will require a Business Associate Agreement (BAA) with Couchbase in order to store and manage PHI in Capella. Customers can enter into a BAA with Couchbase by contacting our Information Security or Sales representatives. This is applicable for Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure.

PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security requirements designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment to protect payment card data. Couchbase Capella has attestation of compliance (AoC) for PCI DSS v4.0, Service Provider Level 1. This is applicable for Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure.



CSA STAR

The Cloud Security Alliance (CSA) is committed to outlining and promoting best practices for ensuring a safe cloud computing landscape. They oversee the Security, Trust, Assurance, and Risk (STAR) Registry. Couchbase has successfully received a CSA STAR Level 2 attestation of compliance, following an external security audit of Capella. This is applicable for Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure.

Identity and access management

The principle of least privilege forms the basis for access management at Couchbase. System administrators and data owners are authorized to access Couchbase resources and sensitive data on a need-to-know basis. Periodic access reviews are performed to ensure compliance with access and authorization policies and to revoke access if no longer required. In addition, processes are in place to remove terminated employees' access on their last working day. Access to systems and resources is reevaluated for employees who change roles. Remote access to Couchbase resources is allowed over secure virtual private networks (VPN) only. Employees must enter their multi-factor authentication token before

accessing production and corporate environments as an added layer of security. Access to company systems or resources is configured with password complexity requirements and unauthenticated access is prohibited.

AUTHORIZATION IDENTITIES

Couchbase Capella distinguishes identities that can access the Control Plane or data in the Data Plane. This is performed using two types of users: Organization Users and Database Users. Organization Users are allowed to access the Control Plane. An Organization User can have administrator privileges and data privileges as well.

Organization data protection

Couchbase has implemented measures and controls to prevent unauthorized read, copy, modification, or removal of sensitive Organization data during transmission or at rest. In addition, communication and Organization data transmissions across networks are allowed only over secure networks using industry-standard encryption protocols.

ENCRYPTION IN TRANSIT

Couchbase does not permit plain text traffic over public networks. Internet-facing production servers and applications use SSL/TLS certificates signed by a known, trusted provider. Couchbase Capella encrypts data in transit using TLS 1.2 or higher encryption which is performed between the Control Plane and the Data Plane, between nodes in the same cluster, and from the Organizations' application to the Data Plane. This ensures the privacy of user data and the integrity of servers and their clients. TLS encryption cannot be turned off.

ENCRYPTION AT REST

All data is encrypted at rest using the native encryption solution offered by the cloud provider chosen by the Organization for the Data Plane, such as Encrypted EBS Volumes in AWS. Couchbase Capella uses Organization master keys that are encrypted using a 256-bit AES algorithm. These symmetric keys are not exportable. A new key is created for each Cluster. Additionally, fields within a JSON document can be securely encrypted at the client-side with functionality built into the Couchbase SDKs known as field-level encryption. This is a great option for the encryption of sensitive fields that may call for a higher level of security. The data is transparently encrypted when writing to Capella and transparently decrypted when reading from Capella using Organization-managed keys. This data is never in an unencrypted state, even while in use within Capella. For more information, please refer to our documentation at **https://docs.couchbase.com/sdk-extensions/field-level-encryption.html.**

SECRETS MANAGEMENT

Couchbase Capella uses the chosen cloud provider's native secrets management functionality (e.g., secrets manager) to securely store secrets such as passwords and certificates. All credentials and secrets are protected by the principle of least privilege and are not accessible to Couchbase employees. Any unauthorized attempt to access by anyone other than an Organization User, including Couchbase or hackers impersonating Couchbase, will result in an audit trail and an immediate

alarm. A fully automated intrusion prevention system is employed to detect and prevent attempts to breach or compromise application containers with access to those credentials and secrets.

CAPELLA CLUSTERS AND DATA SEGREGATION

Each Organization's data is segregated on a separate virtual network to avoid unauthorized access by other Organizations.

Capella isolates Organizations in their own individual cloud accounts. Within that isolated cloud account, Capella Clusters are deployed within its own virtual private cloud (VPC). The Cluster and VPC are tied together and cannot exist without each other. Each cluster exists within its own network and has its own compute and storage.

This Cluster isolation extends to clusters within a Project and also permits alerts and metrics to be defined at the Cluster level. This also permits Users to be assigned at the Cluster level.

Capella network security

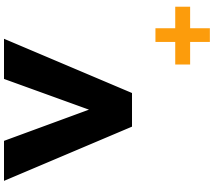
Network segregations restrict communication between networks with different risk profiles. Examples of segregated networks are corporate, development, test, and production networks.

ORGANIZATION ISOLATION

Couchbase Capella is deployed into the cloud provider over a virtual network which allows Organizations to securely build multi-tier web applications and strictly enforce access and security restrictions between their web servers, application servers, and databases. The Couchbase Capella Data Plane provides control over the virtual networking environment and is completely managed by Couchbase. The Couchbase Capella Control Plane is a multi-tenant user interface for the management of databases. User authentication and authorization are linked to a unique and specific Organization account, inaccessible across tenants.

SECURE ACCESS

On Couchbase Capella, the Data Plane accepts the Control Plane IP address by default for monitoring and maintenance purposes. All other IP addresses are rejected for maximum security unless specifically added by the Organization. Using Capella, the environment will be configured by default to allow no inbound access. The Data Plane will only allow its clusters to connect to trusted IP addresses. Any attempted connection from an address that is not on the allowed IP address list will be denied. Allowed IP addresses are configured per cluster and can be configured as a single address or a CIDR block. Allowed IP addresses can also be temporarily added with user-specified expiration times to improve security for short-term access. All communication that occurs with a given Data Plane uses TLS 1.2 or greater as an encryption layer so that attackers cannot snoop the network traffic.



VIRTUAL PRIVATE CLOUD PEERING

By default, all communication with the Data Plane occurs encrypted over the public internet, with access controlled by the allowed IP list. Optionally, Capella provides a private networking mechanism that leverages VPC peering to improve both latency and security of the connection from Organization-managed application VPCs to Capella cluster VPCs. This ensures that the database traffic never traverses the public internet, reducing the potential of common threats such as DDoS attacks. Couchbase Capella does not require outbound network access into the peered application VPC, this mechanism is only used to provide application access to the cluster. As VPC peering is not transitive, Capella will be unable to access other VPCs that are peered to the application VPC. It is suggested for optimum security that you create a unique VPC for your applications connected to a Capella cluster via this mechanism.

DevOps security

PROTECT AND PREVENT ATTACKS

Capella's entire paradigm is built to protect Organizations' data and prevent attacks while providing visibility and control using fully automated intrusion prevention to protect against unauthorized access. This is accomplished using container immutability, hardening of the host, and strict monitoring for anomaly detection and prevention. Container firewalling is also implemented.

CONTROL PLANE ATTACK PREVENTION

The Control Plane is protected by an application firewall to prevent common attack vectors such as cross-site forgery, cross-site scripting (XSS), and remote file inclusion (RFI). Rate limiting is also implemented to prevent DDoS attacks. The Control Plane also prevents parameterized queries to block SQL injection attacks.

DATA PLANE ATTACK PREVENTION

The Data Plane is protected by the underlying security measures of the selected VPC (such as AWS, Azure, or GCP). To prevent traditional SSH attacks, Capella blocks all SSH access. All IP addresses are blocked by default, and the Organization will be required to explicitly whitelist IP addresses via the allow list in the Control Plane. VPC peering is used for secure communication between the Control Plane and Data Plane.

INFRASTRUCTURE HYGIENE

All internal infrastructure is hardened using RBAC, and only essential Couchbase staff has access to important touchpoints. Center for Internet Security (CIS) checkpoints are implemented to safeguard all systems. This includes using minimal operating system implementations, hardening of the OS, and all non-standard ports and privileges are blocked.

PROACTIVE MONITORING

Capella maintains audit trails to capture operations event logs. In addition, this audit data is secured and cannot be modified. Audit trails cannot be bypassed and are designed to capture any modification to the service, including all access permissions and changes to the configuration. Audits capture the ID of the user profile, IDs of

TROUBLESHOOTING LOGS ARE COLLECTED EVERY THREE HOURS AND SECURELY STORED IN AN ORGANIZATION'S DATA PLANE.

the approver of the event, metadata of the event, and date and time of the event. Additionally, comprehensive auditing of access to secrets and whitelisting of IP addresses control database access. This data is maintained as long as the Capella subscription is active.

TROUBLESHOOTING LOGS

Couchbase Capella maintains a centralized log management system that alerts the Couchbase Operations team if there are any concerns. These logs are redacted. Redacted information includes:

- Key/value pairs in JSON documents
- Usernames
- Query fields that reference key/value pairs and/or usernames
- Extended attributes

Logs are collected every three hours and securely stored in an Organization's Data Plane. If a support ticket is created, recent logs are automatically sent to Couchbase Support. Only authorized Couchbase engineers have access to these logs. This allows Couchbase engineers to triage issues.

CAPELLA OPERATIONS MANAGEMENT

Access management is provided to the Cloud Operations team to ensure any ingress to the environment is limited. Under extreme circumstances, Couchbase Operations may be required to access an Organization's Data Plane. If so, the Organization must provide Couchbase explicit permissions to the Organization's environment. This access will expire in one hour and an audit trail will be automatically captured. The approval process for this access is limited to Couchbase staff who have been granted the required preapproved operational roles to access any underlying systems. After the Organization grants this access, Couchbase senior management is also required to approve via an exception process. This secured access requires multi-factor authentication to the environment and is logged to the Cloud Operations team for compliance reasons. Cloud Operations team members are also audited quarterly and any access to systems is revoked upon departure from the Cloud Operations team or the company.

APPLICATION SECURITY AND PENETRATION TESTING

The Couchbase Capella Operations team performs regular independent third-party penetration tests. This allows us to better identify internet-accessible company assets, scan for known vulnerabilities, evaluate risks, and track issue remediations. Findings are documented, tracked, and remediated, if necessary. Internal and external networks, infrastructure systems, and web applications are in the scope of the annual penetration tests.

The engineering teams utilize a secure code development process and a version control system (VCS) for the deployment of code changes, continuous integration (CI), and continuous delivery (CD). Static application security testing (SAST) and software composition analysis (SCA) are an integral part of the development process. Mechanisms are in place to ensure that software releases cannot be deployed to the production environments without a code review and approval.

CHANGE AND RELEASE MANAGEMENT

Changes to software and system configurations are deployed to a non-production environment and tested for acceptance before deployment to production using either automated or manual testing techniques.

The Operations team is routinely involved in source code and architecture reviews, code commit, peer reviews, and modeling of threat and security concerns. Security testing follows OWASP standards and methods, and external parties are used for further review and auditing.

LEARN MORE

Couchbase Capella has been architected and built on three important security pillars: Verify Explicitly, Least Privilege, and Platform Monitoring. Capella, as a technology and as a service, delivers a secure data environment for Organizations with the highest form of data isolation in the cloud, stringent access protection with authentication and authorization controls, and a tightly locked down data plane infrastructure.

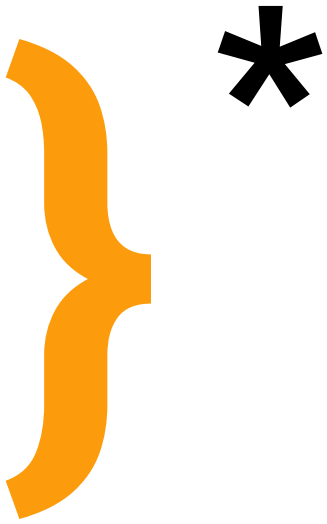
We know security is a critical aspect of Database-as-a-Service and that Capella will deliver for Organizations in this area.

Capella resources

- Product information: https://www.couchbase.com/products/capella
- Documentation: https://docs.couchbase.com/cloud/index.html

Want to try Capella?

Sign up for a 30-day free trial: https://cloud.couchbase.com/sign-up



Modern customer experiences need a flexible database platform that can power applications spanning from cloud to edge and everything in between. Couchbase's mission is to simplify how developers and architects develop, deploy and consume modern applications wherever they are. We have reimagined the database with our fast, flexible and affordable cloud database platform Capella, allowing organizations to quickly build applications that deliver premium experiences to their customers—all with best-in-class price performance. More than 30% of the Fortune 100 trust Couchbase to power their modern applications.

For more information, visit www.couchbase.com and follow us on Twitter.