druva

White Paper

Druva Phoenix: Enterprise-Class Data Security & Privacy in the Cloud

Advanced, multi-layer security to provide the highest level of protection for today's enterprise.

druva

White Paper

Table of Contents

Overview

With Druva, you can rest assured that your enterprise's data is completely secure end to end. Druva comprehensively protects your corporate data by adhering to strict standards that keep your data private and safe from external threats. With data protection as its number one priority, Druva's solutions are engineered to ensure data security at every step: transmission, storage, and access.

This document is designed to provide a more detailed review of the security guidelines and measures that Druva has put in place to protect customer data. As will be shown, Druva's data security takes a multifaceted approach that extends far beyond basic encryption.

Cloud Security

At Druva's foundation is a core service that provides connectivity to your servers for data storage and retrieval. Within this service, data is handled following these methods:

Data in Transit

Druva is designed from the ground up with the understanding that servers often connect over WANs and VPN-less networks for backup activities. The Druva service always encrypts data in transit with 256-bit TLS encryption, ensuring enterprise-grade security over these networks.

Data at Rest

In addition to strict authentication and access controls, Druva secures data in storage with 256-bit AES encryption. The keys used are unique to each customer and utilize a two-factor encryption mechanism to obfuscate the key. Additionally, no data is shared between customers.

Secure Server Registration

Servers are registered through a token based method which gives administrators the ultimate control over when and how servers are added to the solution. Server registration can be as tightly controlled as needed.

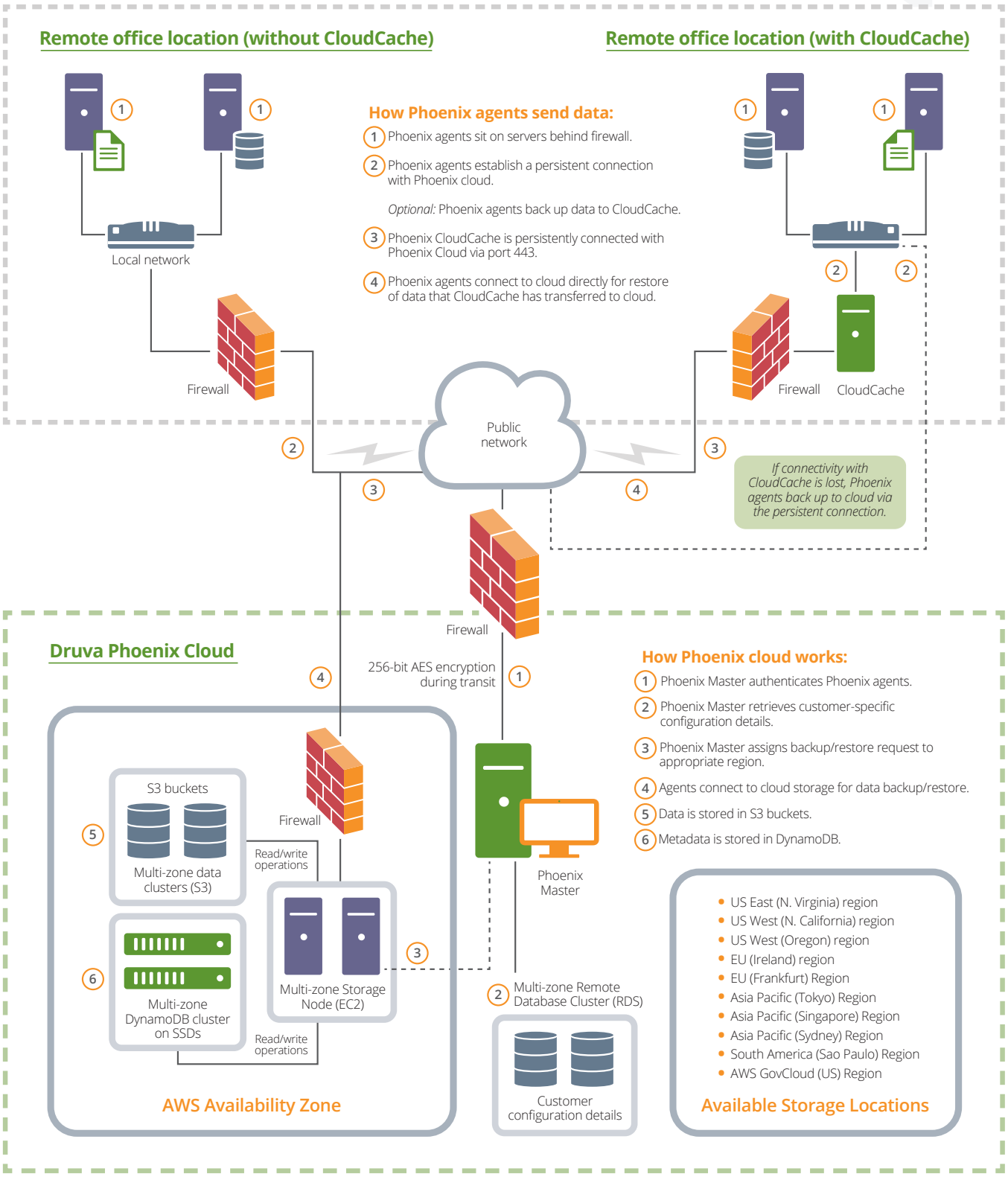
Druva's Cloud Services

Druva Cloud is a fully-automated, enterprise-class data protection solution offered as a software as a service (SaaS). Powered by Amazon's state-of-the-art AWS technology, Druva Cloud offers elastic, on-demand storage that can grow to handle any number of servers with any amount of data. The service can be instantly provisioned to a global base with policies that lock storage to specific regions.

Druva Cloud offers secure, lightning-fast data backups and restores. It operates within multiple storage regions across the world to address the needs of the global enterprise. The service provides high availability and enterprise-scale RPO and RTO. The service's enterprise-class infrastructure is compliant with international standards such as ISO-27001, SOC-1, SOC-2, and SOC-3.

Full administrative control of Druva Cloud is provided via a secure Web-based administrator control panel over HTTPS, which allows corporate policies to be defined for servers. Specific management rights can be delegated to specific administrators, allowing them to see and manage only their devices, without visibility into other data within the organization.

On the client side, the device agent is a lightweight, non-intrusive application that manages data backup. It can be provisioned in a two step process, which is easily scripted for mass deployment scenarios.


Remote office location (without CloudCache)
Remote office location (with CloudCache)
How Phoenix agents send data:
1 Phoenix agents sit on servers behind firewall.
2 Phoenix agents establish a persistent connection with Phoenix cloud.
Optional: Phoenix agents back up data to CloudCache.
3 Phoenix CloudCache is persistently connected with Phoenix Cloud via port 443.
4 Phoenix agents connect to cloud directly for restore of data that CloudCache has transferred to cloud.
Local network
Firewall
Firewall
CloudCache
Public network
If connectivity with CloudCache is lost, Phoenix agents back up to cloud via the persistent connection.
Firewall
Druva Phoenix Cloud
256-bit AES encryption during transit
How Phoenix cloud works:
1 Phoenix Master authenticates Phoenix agents.
2 Phoenix Master retrieves customer-specific configuration details.
3 Phoenix Master assigns backup/restore request to appropriate region.
4 Agents connect to cloud storage for data backup/restore.
5 Data is stored in S3 buckets.
6 Metadata is stored in DynamoDB.
S3 buckets
Multi-zone data clusters (S3)
Firewall
Read/write operations
Phoenix Master
Multi-zone Storage Node (EC2)
Multi-zone DynamoDB cluster on SSDs
Read/write operations
Multi-zone Remote Database Cluster (RDS)
Customer configuration details
AWS Availability Zone
US East (N. Virginia) region
US West (N. California) region
US West (Oregon) region
EU (Ireland) region
EU (Frankfurt) Region
Asia Pacific (Tokyo) Region
Asia Pacific (Singapore) Region
Asia Pacific (Sydney) Region
South America (Sao Paulo) Region
AWS GovCloud (US) Region
Available Storage Locations

Flexible Data Retention

Druva Cloud enables its customers to hold infinite restore points for protected data. Administrative control provides the ability to specify file retention at backup policy level. If this option is chosen, an automatic process, called compaction, runs daily to remove any data outside of the retention rules. Administrators with appropriate rights also have the ability to selectively remove restore points for individual servers where required.

Druva Cloud Security Objectives

Druva strictly adheres to the following set of objectives to ensure the security of our cloud service:

- Ensuring data security during bidirectional transfer between servers and cloud infrastructure
- Segregation of customer data
- Two-factor encryption key management and authentication
- Data center security
- Additional security mechanisms to protect Cloud infrastructure and data assets
- Third-party security verifications ISAE-3000 and HIPAA

Segregation of Customer Data

Druva Cloud segregates each customer's data from other customers' data, thereby resulting in a virtual private cloud for each customer.

Virtual Private Cloud for each customer is realized by:

- Compartmentalization of customer configuration based on access credentials
- Compartmentalization of customer metadata within Dynamo DB
- Compartmentalization of customer data within S3 buckets
- Encrypting data of each customer using a unique 256 AES encryption key

Two-Factor Encryption Key Management & Authentication

To uphold the highest security standards for enterprises, key management in the Druva Cloud is modeled after a bank lockbox system, in which both parties hold part of the key. The encryption and authentication keys are mutually shared between the customer and the Cloud. Consequently, neither has full, unencrypted access to any data on the cloud independently.

Key Points to Note:

Both authentication and encryption depend upon two pieces of information:

- Admin password (held ONLY by the customer)
- Encryption token (held ONLY by Druva)

Both these pieces are required to authenticate the user and get the unique account key, which is used to encrypt and decrypt server data. This is otherwise known as the AES-256 encryption key.

At no time is the actual key saved by the server; it exists only at the time a server or admin is authenticated, used in working memory for the duration of the session, and is then destroyed.

This strict key management mechanism ensures that:

1. **Druva NEVER has access to your data.** If required to present your data to a third party (for example, to the federal government), we CANNOT do so.
2. **Druva CANNOT reset your password.** Since the admin password is needed to construct the key required to decrypt the data, we require that the user set up multiple administrators. If a password is forgotten by any of the administrators, one of the other administrators in the organization can reset it. Druva CANNOT do so.

Druva Security Model

Client Initiated Architecture

With Druva Phoenix, all connections are initiated by the server agent, which aids in security and scalability of the server. The Druva service never initiates any client connections, and a single port is used for all configuration, control and data requests. All communication is secured using 256-bit TLS encryption.

Creation of Customer Environment and Encryption Key

1. Cloud admin logs into the system for the first time with account A1 using password P1.
2. A random key is generated (AK), which is an AES 256-bit key used for encryption of customer data. This is unique per customer.
3. A security token is created using a hash of the administrator's password and the newly created AES encryption key. The formula for the creation of this key is as follows: New Token T1 = AK + P1 + salt, where salt is a random string generated for this operation.
4. This token is saved in the cloud, while the password is held only by the admin.
5. Additional administrator accounts can be created by an existing administrator through a similar process.

Neither the administrator's password nor the hash of the administrators password is stored in the Druva Cloud at any time. Due to the nature of the security model, if all administrator passwords are forgotten there is no way to access customer data. In order to provide complete data privacy to our customers, Druva is unable to reset admin passwords under any circumstance.

Process for authenticating an administrator

1. Admin enters password for login.
2. Hash of password is calculated and attempt is made to decrypt the the encryption key (AK).

3. If AK decryption is successful and returns a valid value, the admin is logged into the system. This validates that only an administrator is allowed to connect to the system and access data, and can be done without storing the admin password in the Druva cloud.

Process for registering a server agent

Registering a Phoenix agent with a specific Phoenix environment is very straightforward.

1. A random number token is generated.
2. A SHA-256 hash of this random number is made.
3. The hash and unique account key are encrypted using the hash value itself and stored on the Druva Cloud, as an encrypted token (eToken). The encrypted token is shown to the administrator in the web UI, where it can be copied but is not available anywhere else.
4. To register a server, an admin supplies the token during the activation process. This token is used to decrypt the encrypted version of the encryption key held on the server. If the decryption is successful, this allows the client to be successfully registered.
5. A device specific key is created and stored on the server. The encryption key (which was unencrypted into working memory on the server in the previous step) is encrypted using the hash of the device key and stored in the Druva Cloud.

Process for connecting agent for backup/restore

1. Server connects to Druva cloud using the device specific key.
2. Attempt is made using device key to decrypt the encryption token (AK). If token can be successfully decrypted, the server is authenticated.
3. Data can be sent and retrieved from the cloud storage environment.

Process for restoring data

1. Admin queues a restore request from an existing server snapshot.
2. Druva Cloud relays the admin request to the server agent.
3. Server agent starts the restore process.

Phoenix Cloud Management Control Panel

- Administrative access to each Phoenix instance is provided via an Admin Control Panel.
- Phoenix Cloud does not store the admin password but uses the authentication methodology defined in section above.
- An administrator can create multiple other admins based on roles. There are two primary types of administrators:
  - Cloud administrator: Has overall administrator rights across all areas of service
  - Group administrator: Has delegated access to specific server groups. Cannot see the data and activities of servers outside these groups.
- No Druva employee has any level of administrator access to the instance.
- Only Cloud administrators can revoke access of another admin at any time by removing the appropriate admin account via the web-based admin control panel.

Phoenix Cloud Access by Druva Employees

Druva employees have no access to any of a customers' instances. Access to cloud infrastructure by Druva employees is limited to its cloud operations team that follows strict rules and regulations defined under the Druva security policies document. This access is granted for the purpose of security patching, service upgrades, and monitoring tasks.

Data Center Security

Druva Cloud is built on top of the Amazon Web Services (AWS) technology stack. Amazon has several years of experience in designing, constructing, and operating large-scale data centers. AWS infrastructure is housed in Amazon-controlled data centers throughout the world. Only those within Amazon who have a legitimate business need to have such information know the actual location of these data centers, and the data centers themselves are secure and meet ISO-27001, SOC-1, SOC-2, and SOC-3 certification requirements.

The AWS network provides significant protection against network security issues including (but not limited to):

- Distributed denial-of-service (DDoS) attacks
- Man-in-the-middle (MITM) attacks
- IP spoofing
- Port scanning
- Packet sniffing by other tenants

For details, please refer Amazon Web Services - Overview of Security Processes at **www.aws.amazon.com/security/**.

Additional Security Mechanisms to Protect Cloud Infrastructure and Data Assets

Redundancy

AWS data centers are designed to anticipate and tolerate failure while maintaining service levels and are built in clusters in various global regions. The Druva Cloud provides multi-zone replication of various elements of customer data including configuration, metadata and the actual data, thereby ensuring that customer data is available in multiple availability zones to handle failure of any zone.

Redundancy measures provided by Amazon include (but not limited to):

- Fire detection and suppression
- Power
- Climate and temperature
- Management

For details, please refer Amazon Web Services - Overview of Security Processes at **www.aws.amazon.com/security/**.

Third-Party Security Certifications

Above the certifications held by Amazon as an infrastructure provider, Druva has undergone a number of third party audits as a solution provider.

ISAE 3000 Type II

Druva Cloud Operations undergo a bi-yearly ISAE 3000 Type II certification by KPMG. The ISAE audit covers the following elements:

- Description of Druva's system related to general operating environment supporting Druva Cloud Operations.
- Design of controls related to the control objectives stated in the description.

HIPAA

Druva has passed a review by KPMG validating the company's security and privacy controls for handling HIPAA-compliant protected health information (PHI).

TRUSTe EU Safe Harbor

Druva has achieved TRUSTe EU Safe Harbor certification facilitating compliance with the European Union's Data Protection Directive.

These certifications are available from Druva upon request.

About Druva

Druva is the leader in data protection and governance at the edge, bringing visibility and control to business information in the increasingly mobile and distributed enterprise. Built for public and private clouds, Druva's award-winning inSync and Phoenix solutions prevent data loss and address governance, compliance, and eDiscovery needs on laptops, smart devices and remote servers. As the industry's fastest growing edge data protection provider, Druva is trusted by over 3,000 global organizations on over 3 million devices. Learn more at **www.Druva.com** and join the conversation at **twitter.com/druvainc**.

druva

Druva, Inc.
Americas: +1 888-248-4976
Europe: +44.(0)20.3150.1722
APJ: +919886120215
sales@druva.com
www.druva.com

Q216-CON-10520