druva

White Paper

INSYNC ENTERPRISE-CLASS SECURITY

Advanced, multi-layered security that delivers the highest level of protection for today's enterprise

Q418-CON-10841

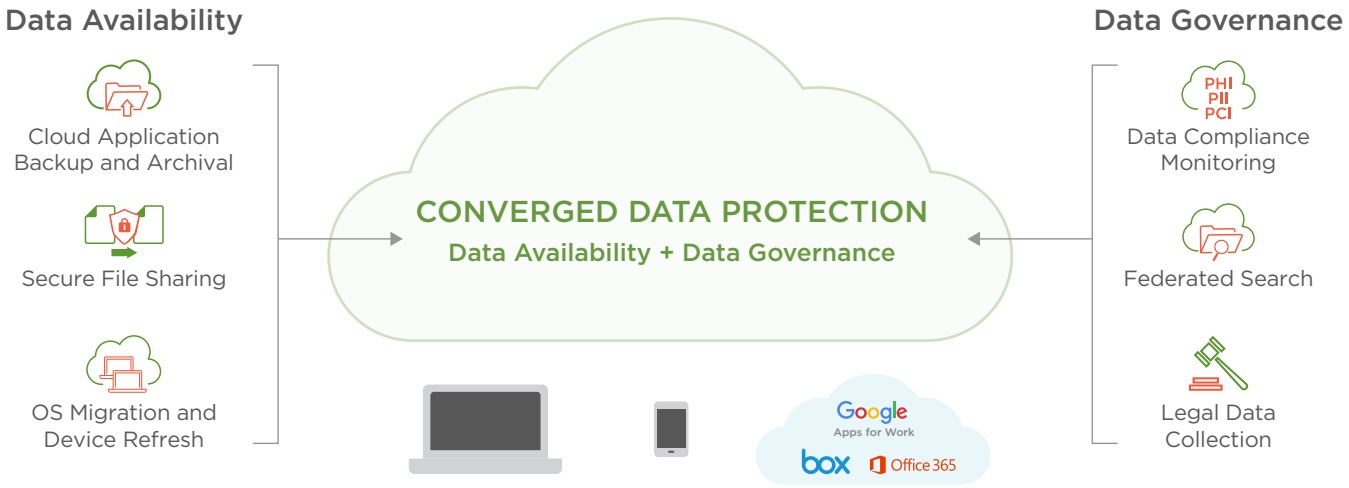
Executive Summary

Druva keeps enterprise data completely secure from end to end by adhering to proven standards that protect your data's privacy and safeguard it from external threats. Developed with security as a foundational cornerstone, Druva's solutions are engineered to ensure data protection at every step—transmission, storage, and access.

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

inSync Overview

inSync provides converged data protection for today's mobile workforce. For IT, inSync offers rich solutions like mobile data backup, data loss prevention and tamper-proof audit trails for eDiscovery. For end users, inSync provides self-restore capabilities and anytime, anywhere, any-device access and sharing.



inSync's mobile application allows users to access backed-up and shared data from any of their mobile devices while providing administrators a variety of policy options to protect devices and data on corporate-owned, as well as BYOD, devices.

Druva Cloud Services Overview

inSync Cloud is a fully-automated, enterprise-class endpoint protection solution offered as software-as-a-service (SaaS). Powered by state-of-the-art technology from AWS, inSync Cloud offers elastic, on-demand storage that can grow to accommodate any number of users and data. And, inSync Cloud can be instantly provisioned to a global user base with policies that lock user storage to specific regions.

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

Full administrative control over inSync Cloud is provided via a secure Web-based administrator control panel over HTTPS. This allows corporate policies to be defined for groups of protected users, including whether those users have the ability to change settings on their accounts.

On the client side, the inSync Cloud agent is a lightweight, non-intrusive client application that manages data backup along with other endpoint services, such as DLP and file sharing, on each protected device.

Empowered with centralized policy-setting controls, IT can enable end users to manage their preferences—such as folder selection and scheduling—while also providing them access to their shared and backed-up data, including data from their other devices.

Druva Cloud Security

In order to secure customer information in the cloud, Druva implements a multi-tiered security model. The components of that security model are defined in this section.

Secure Multi-Tenancy

The Druva Cloud provides a secure, multi-tenant environment for customer data, thereby resulting in a virtual private cloud for each customer.

This secure multi-tenancy 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-bit AES encryption key

Data In Flight

Druva is designed from the ground up with the understanding that endpoints often connect over WANs and VPN-less networks for backup activities. The Druva service always encrypts data in transit with 256-bit TLS 1.2 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 data encryption keys used are unique to each customer and utilize an envelope encryption mechanism to protect the data encryption key itself. The use of a unique encryption key per customer creates crypto-segmentation between customers, preventing data leakage.

Network Security

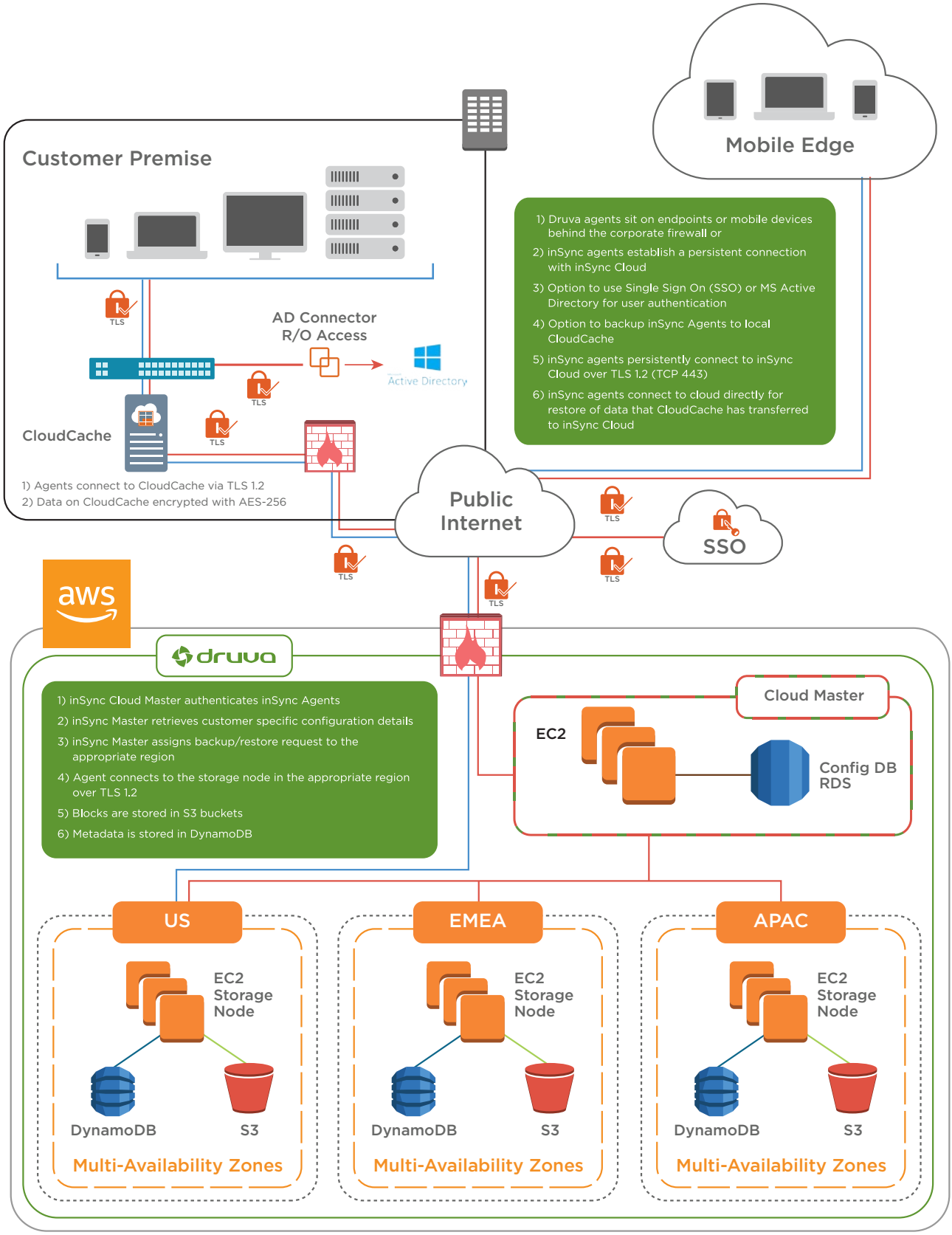
Above and beyond the security mechanism that Druva provides as part of the inSync SaaS offering, the AWS network includes significant protection against network security issues, including (but not limited to):

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

For details on the security provided by Amazon Web Services, visit www.aws.amazon.com/security/.

inSync Architecture

This diagram shows an overview of the inSync architecture, including its security capabilities:



inSync Architecture Components

Druva inSync is comprised of multiple components that, when combined, provide complete protection of customer information. Those components are as follows:

Cloud Service Providers

Druva Cloud, where the inSync SaaS application resides, is built on top of the Amazon Web Services (AWS) technology stack. Amazon has significant experience in designing, constructing, and operating large-scale data centers. AWS infrastructure is housed in their respective organizations' 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.

Cloud Master

The Druva Cloud Master for inSync sits in Amazon Web Services inside the Druva Virtual Private Cloud (VPC). The Cloud Master provides a variety of services for the Druva Cloud. At a core level, the primary function of the Cloud Master is to provide customer-facing Web User Interface services to our customers. Relative to security, these services include authentication of administrators, end users, and endpoints. The Cloud Master allows customers to manage configuration data of their cloud instance for backup, as well as designate in which region the information is stored, enabling Disaster Recovery as a Service (DRaaS).

Cloud Cache

inSync CloudCache is a dedicated server that stores data from inSync agents, then periodically synchronizes this data to inSync Master. inSync CloudCache is deployed within the perimeters of customer data centers and other locations. This ensures that inSync agents can connect to inSync CloudCache via LAN, thus accelerating backups and restores of local data. inSync CloudCache provides local data caching to achieve LAN-speed backup and recovery. With its flexible scheduling and cache controls, CloudCache delivers hot snapshots (up to 30 days) on-premises while efficiently utilizing your WAN bandwidth to the cloud.

Endpoint Agents

Druva inSync provides a single pane of glass for managing data availability and information governance across endpoints and cloud applications—enabling businesses to mitigate data risks and facilitate business continuity while not impacting employee productivity. Effectively protecting endpoint data requires smart integration with multiple flavors of endpoints.

inSync provides the following agents for your heterogeneous server environments:

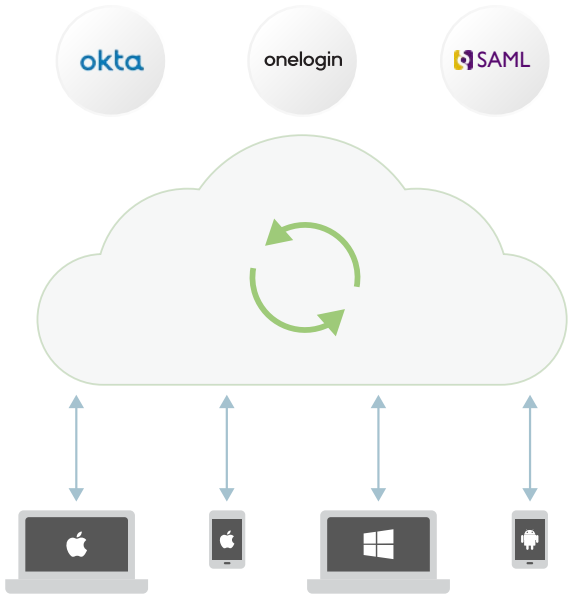
- Microsoft Windows
- Mac OS X
- Ubuntu
- CentOS
- Apple iOS
- Android
- Windows Phone

Enterprise Security

A key consideration is how a product will integrate into an existing enterprise environment. This section describes how inSync integrates into an existing security infrastructure.

Single Sign On

inSync Cloud supports SAML, an XML-based open standard for exchanging authentication and authorization data between security domains. SAML permits users to securely log into inSync using their credentials on external identity services such as Microsoft Active Directory Federation Services, or other third-party providers like Okta and OneLogin.



Active Directory Integration

inSync's Cloud AD connector extends all the benefits of deep AD integration to inSync Cloud, enabling integrated mass deployment of the inSync client, automatic user provisioning and deprovisioning, user authentication, and user management.

Audit Logging

Traceability of security events on any device is a standard requirement in any regulated environment. inSync supports the use of audit logging of security events for both users and administrators, no matter what device they're using. Audit logging for inSync is done in real time, on an event-driven basis, complete with time and date stamping. The audit logs can be stored on the system based on customer requirements and can be downloaded for additional analysis in CSV or HTML format.

Role-Based Access Control

In order to prevent privileged users from making unauthorized changes to resources within their own instance of the Druva SaaS applications, both inSync and Phoenix have implemented a role-based security capability. This capability allows organizations to limit privileged user access to a predefined set of roles and data assets. This RBAC capability makes it possible to create ethical walls to enforce privacy, as well as implement a delegated administration structure to meet customers' organizational, compliance, or security requirements.

inSync supports the following Role-Based Access Control Scheme:

Role	Duties
Cloud Admin	An administrator assigned to this role can perform all core inSync activities, such as configuring, managing, and monitoring inSync. A cloud administrator can create and manage other administrators. Only cloud administrators can manage a cloud administrator. Only cloud administrators can configure a compliance policy. They can also place and view users on legal hold.

Data Protection Officer	An administrator assigned to this role has the necessary permissions to manage data privacy and data access settings for inSync users. The data protection administrator cannot place or view users on legal hold.
Help Desk Admin	An administrator assigned to this role has the necessary permissions to manage day-to-day activities such as performing backup and restore operations, resetting user passwords, and addressing user complaints. The help desk administrator cannot place or view users on legal hold.
Legal Admin	An administrator assigned to this role can perform activities related to legal hold, such as creating and deleting legal hold policies, viewing users who are on legal hold, adding and removing users from legal hold, and viewing and accessing backed-up data.
Profile Admin	An administrator assigned to this role has the necessary permissions to manage users and devices, as well as backups and restores. Profile administrators can access the non-compliance report only for the profiles that they are mapped to. However, they cannot view the compliance summary at the Compliance Dashboard, or configure a compliance policy. Profile administrators cannot place or view users on legal hold.
View-Only Admin	An administrator assigned to this role has the necessary permissions to view inSync settings and user details. They also have access to inSync reports. The view-only administrator cannot place or view users on legal hold.

Endpoint Security

inSync includes a simple but highly effective solution that reduces the economic impact of a lost or stolen endpoint on an enterprise. Device-level security features provide powerful, multilayered protection of critical corporate data on endpoints. With inSync, critical files and folders on laptops and mobile devices can be selected for data encryption to ensure they are protected with the highest encryption standards.

Endpoint Authentication

All endpoint access to inSync is authenticated using device keys that are unique to that device. Device keys are issued to endpoints upon registration by an end user or an administrator. How and when devices are registered is controlled by profile policy. Once issued, when an endpoint attempts to access inSync, the device key is presented to the Druva Cloud Service via transport in a TLS 1.2 encrypted tunnel and authenticated.

Policy-Based Access

Access to inSync data on mobile devices is enabled at a profile level that is assigned to a user. Allow mobile access to corporate data only to a select group of employees, based on their roles, privileges and security levels, or based on which projects they're working on.

By making it a profile setting, inSync provides the option to allow only select employees' mobile access to corporate data based on their roles, privileges, and security levels—or even based on the projects they work on.

Containerization

inSync recognizes that IT administrators need to have control over corporate data stored on all endpoints, including company-owned devices and employee-owned (BYOD) devices. To help administrators achieve this, inSync employs a private container that allows administrators to wipe critical data in a compartmentalized manner.

Data In Flight Security

Communication between the endpoint and inSync is encrypted using 256-bit, TLS 1.2 encryption. This ensures that data at all levels is secure until it is received by the device and presented to the authenticated employee using the the inSync mobile app.

Data At Rest Security

inSync ensures that no data is stored in an unencrypted form on endpoints. Administrators can specify encryption policies for data stored on endpoints as part of their organization's DLP policies. Data is encrypted using AES, leveraging the endpoint operating system's native encryption algorithms. This solution offers much better performance than application-level encryption algorithms.

Remote Wipe

In order to prevent data breach on lost or stolen devices, inSync provides remote wipe capabilities across laptops and smart devices that can be executed either by an administrator or an auto-delete policy. The remote wipe capability uses sanitization techniques to ensure data is unrecoverable from the device in adherence to standards such as NIST SP 800-88.

Geolocation

If a device is lost or stolen, inSync provides the ability to track the geographical location of devices with an accuracy of approximately 20 meters at any point in time. Druva's device geolocation uses advanced hybrid positioning algorithms based on data from Wi-Fi access points, GPS satellites, and cell towers to keep track of all your endpoints. When tracking devices, InSync provides details such as street, city, state, or country in a familiar Google Maps interface for every endpoint device available on the inSync management console.

Backup Security

With inSync's client-triggered data protection architecture, backup and restore requests are always initiated by the inSync client, which aids in security. The servers never initiate any request, and both backup and restore use the same port for all configuration, control and data requests (default 443). All backup and restore activities are secured using a TLS 1.2 connection.

Client-Triggered Architecture

With Druva inSync, backup and restore requests are always initiated by the inSync client, which increases security and scalability of the server. The servers never initiate any request, and both backup and restore use the same port for all configuration, control and data requests (default 443). All backup and restore activities are secured using 256-bit TLS 1.2 encryption.

File Sharing

inSync's security capabilities encompass data synced/shared using inSync Share. inSync Share offers administrators the ability to configure policies for sharing data within the enterprise or data carried by external users. In addition, all shared data is encrypted on the wire, on the server, and also on the endpoints with the DLP option.

inSync provides IT with three-tiered control over shared data within the enterprise:

- User-Level Sharing—Control on employees who can share data
- File-Level Sharing—Control who can share and what can be shared
- External Party Sharing—Centralized control on sharing data with external partners and collaborators

Additionally, inSync offers administrators visibility into data sharing activities and access at all levels to monitor and check for any unsecure sharing practices.

Retention and Version Control

inSync Cloud enables its customers to preserve infinite restore points for protected data. Administrative control provides the ability to specify file retention at an individual backup policy level. If this option is chosen, an automatic process called compaction runs daily to remove any files which lie outside of the retention rules.

Administrators with appropriate rights also have the ability to selectively remove restore points from individual accounts where required. End users of the system have no control over removal of stored files, thus keeping the ownership of protected data with the administrator.

Proactive Compliance

Data dispersed across mobile and cloud apps has dramatically increased the chance of costly data exposures in the enterprise. inSync is the only integrated solution that brings visibility to end user data and provides an automated system to proactively track, monitor and generate notifications of potential data security risks.

Single View of All Your Data

inSync merges data and audit trails across disparate data sources and provides a single monitoring dashboard for viewing and managing end user data without having to scour across multiple disjointed systems — enabling real-time monitoring of all users, policies, and file types for potential non-compliance.

Compliance Automation

By automating the process of identifying files that may contain sensitive information such as personal health information (PHI), personally identifiable information (PII), personal credit information (PCI) and confidential Intellectual Property (IP), inSync provides a unified way for IT to quickly assess and take corrective action for non-compliance on regulated or policy-managed end user data.

Secure Discovery and Response

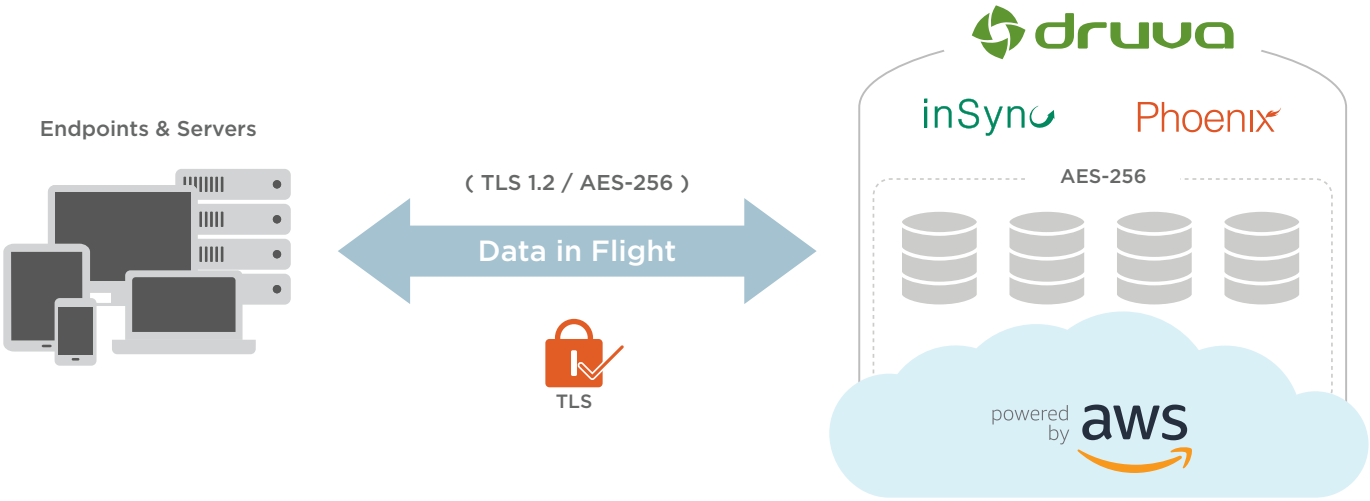
When required for investigative, compliance or legal requirements, inSync captures extended metadata (as outlined by the Department of Justice) and creates a unique signature for every file in the system. In doing so, inSync is able to provide an auditable trail of a file's history and a litmus test for its authenticity. inSync is also the only solution available today that enables organizations to explicitly hold data and provide direct access to investigative or compliance teams without end user involvement. Not only does this streamline the data hand-off process, minimizing spoliation risks, it also ensures discretion during sensitive audits.

Data Encryption

A key attribute of any cloud service is the ability to secure data both "in flight" and "at rest." All data that Druva sends to the cloud is protected in flight to AWS using industry-standard Transport Layer Security (TLS). Data at rest, whether it's stored on the customer premises in the inSync CloudCache or in the Druva Cloud Service storage node, is protected with AES 256-bit encryption. The following is an in-depth look at the Druva encryption architecture.

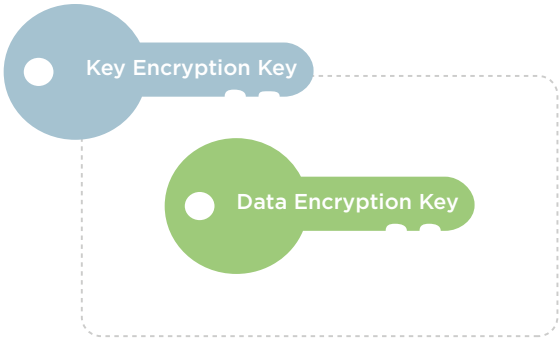
Encryption Overview

Once the data arrives in the Druva Cloud Service at the pre-defined regional storage node over a TLS 1.2 connection, it is immediately encrypted using an AES 256-bit encryption key that is unique to, and completely controlled by, that customer. The following diagram illustrates the encryption flow.



Druva has no access to this encryption key or customer data. This unique encryption key per customer guarantees that in addition to the logical separation, there is an additional layer of access control that prevents data leakage in the cloud for data at rest. This customer encryption key is a session-only key algorithm modeled on digital envelope encryption. The result is that the customer key is never stored, transferred or accessible from outside a user's active cloud-side session, removing the need for expensive and complex key management solutions.

Digital Envelope Encryption



To uphold the highest security standards for enterprises, encryption key management in the Druva Cloud is modeled after digital envelope encryption. Digital envelope encryption is the default standard for cloud encryption. Digital envelope encryption is comprised of two encryption keys, as seen in the following diagram:

The first key is the Data Encryption Key (DEK), which is used to encrypt customer data in the form of unique data blocks stored in S3. This is a randomly generated OFB-AES-256 encryption key that is unique to that individual customer. The DEK is only exposed within the Druva Cloud Service for encrypted I/O operations in volatile memory space. At no time is it exposed in plain text form via WebUI or CLI to either the customer or Druva personnel.

The DEK is generated at the time of the creation of the customer instance in the Druva Cloud Service and stored as an encrypted token in an AWS RDS database. The process for the creation of the DEK and token is as follows:

1. Upon the creation of new cloud instance three things take place:
    a. AES 256-bit encryption is randomly generated (DEK).
    b. An 11-character complex password is generated and delivered to the customer administrator (P1).
    c. Random salt is generated (S1).

2. These three pieces of data are then concatenated (S1+DEK+P1).
3. This concatenation is then AES 256-bit-encrypted with the SHA2 of the randomly generated password (P1) in a Password-Based, Key Derivation Function (PBKDF). This creates the first cloud admin token (AT1).
4. The token is then stored in the RDS database, while the password is held by the administrator.

For additional security, the RDS database where the token is stored is also encrypted using AES-256. At no time is the actual data encryption 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, then destroyed.

The second key is the Key Encryption Key (KEK), also commonly referred to as a Key Wrapping Key (KWK) in the cryptography community. The KEK places the DEK in an encrypted envelope when it is stored as a token in the Druva Cloud Service. The KEK is generated using a Password-Based, Key Derivation Function (PBKDF) by taking the user password or device key and running it through a SHA-256 hash function, which then generates the KEK. This KEK is then used to encrypt the token as described earlier in this section.

At no time is the actual DEK 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, then destroyed.

This strict key management mechanism ensures that:

- **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.
- **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.**

Data Sharding

In addition to digital envelope encryption, another layer of security is derived from Druva's patented deduplication technology, where files are split into individual blocks and only unique blocks are sent to the service globally across all devices. These unique blocks are stored in object storage without any identifying metadata, while block reference data and associated source file metadata are stored in a separate object-based NoSQL database. Doing this ensures that the underlying data is completely obfuscated. Reconstitution of data is only possible through authenticated customer credentials, which are required to instantiate the session-based key mechanism.

The result of this encryption of unique blocks is that the data is sharded, scrambled, and stored within the environment in a manner that makes it impossible for someone to decrypt and reassemble the information without authenticated customer credentials.

CloudCache Encryption

Druva's inSync CloudCache (ICC) is an optional software appliance that can be deployed onsite and offers the most effective Cloud deployment approach for the backup and restore of large data sets in bandwidth-constrained environments. While this software appliance lives on customer premises, the need to protect customer information is just as great as it is in the cloud environment.

The inSync CloudCache encrypts data that is stored on the cache using AES-256 encryption. This encryption key is a different Data Encryption Key (DEK) than the key used to store data in the inSync Cloud.

Operational Security

Druva employees have no access to any of a customers' instances. Access to cloud infrastructure by Druva employees is limited to the cloud operations team that adheres to strict rules and regulations defined under

the Druva security policies document. This access is granted to enable the successful completion of security patching, service upgrades, and monitoring tasks.

Business Continuity

Built in clusters across a variety of global regions, AWS data centers are designed to anticipate and tolerate failure while maintaining service levels. 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 accessible from multiple availability zones, to mitigate the failure of any single zone.

Third-Party Certifications

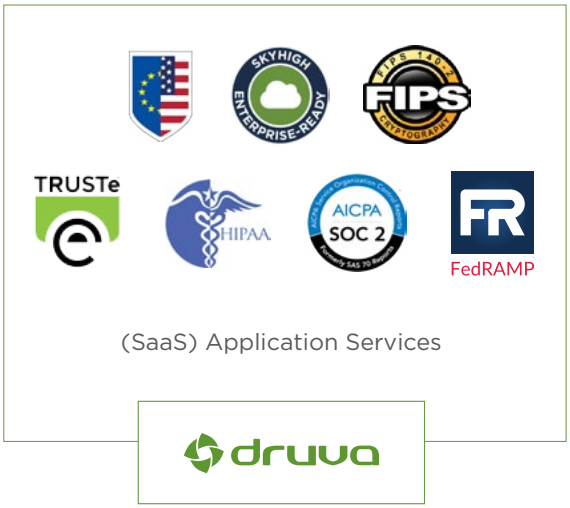
In addition to the certifications held by Amazon as the infrastructure provider, Druva has undergone a number of third party audits as a solutions provider.

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).

These certifications are available from Druva upon request.

About Druva

Druva is the global leader in Cloud Data Protection and Management, delivering the industry's first data management-as-a-service solution that aggregates data from endpoints, servers and cloud applications and leverages the public cloud to offer a single pane of glass to enable data protection, governance and intelligence—dramatically increasing the availability and visibility of business critical information, while reducing the risk, cost and complexity of managing and protecting it.

Druva's award-winning solutions intelligently collect data, and unify backup, disaster recovery, archival and governance capabilities onto a single, optimized data set. As the industry's fastest growing data protection provider, Druva is trusted by over 4,000 global organizations, and protects over 40 petabytes of data. 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) 203-7509440
India: +91 (0) 20 6726-3300
Japan: +81-3-6890-8667
Singapore: +65 3158-4985
Australia: +61 1300-312-729
sales@druva.com
www.druva.com