druva

White paper

Druva security overview

End-to-end data security

Q122-20248

At Druva, security is foundational to all of our development efforts. Druva maintains an enterprise security program to meet the stringent security requirements of our diverse customer base. We make the security of our customers' data the number one priority at every product phase, throughout the development lifecycle, and during backup operations.

Your organization is tasked with ensuring data security, regardless of how or where backup solutions are deployed. Whether extending your existing data center or leveraging SaaS applications as part of a cloud-first strategy, data security is paramount. This is true regardless of whether your backup deployment is on-premises, via the cloud, or as a hybrid model. Choosing the power of the cloud doesn't result in lessened security; at rest or in flight, your data is protected by the security and data governance tools Druva provides.

Unlike traditional approaches, Druva Cloud Platform is built on AWS and offered as-a-Service, with inherently strong security. AWS provides a mature, cloud-based infrastructure, and its platform is globally ubiquitous. Security at an infrastructure level remains constantly on-duty, allowing organizations to access cloud data whenever, wherever. By freeing themselves from the burden of unnecessary hardware, capacity planning, and software management, customers are able to drive down costs by up to 50 percent.

Protect data from loss or compromise, anywhere

The amount of data stored in and used from the cloud is rapidly expanding, while end users are increasingly accessing that data from mobile devices. Smartphones and tablets, in conjunction with the cost savings and elasticity of the cloud, are stretching—if not completely dissolving—traditional security perimeters. This dissolving of the traditional security perimeter makes it absolutely mandatory for data to be secure and recoverable no matter where it lives. Druva's cloud-native architecture and data loss prevention (DLP) capabilities take this new security paradigm into account, empowering organizations to protect data with:

- Flexible backup and recovery solutions that protect data from loss or compromise
- Remote device encryption and sanitization capabilities to prevent data breach
- Geolocation capabilities to aid in device recovery
- Geofencing that can restrict access to data from specific IP addresses or locations

Protecting data in flight and at rest

Customers trust Druva to protect their information no matter where it resides. A key attribute of any cloud service is to be able to secure data both "in flight" and "at rest." To protect data in flight, Druva uses industry-standard Transport Layer Security (TLS) for all data transmitted to the Druva Cloud Platform.

Once the data arrives in the Druva Cloud Platform, it's immediately encrypted using an AES 256-bit encryption key that is unique to, and completely controlled by that customer. Druva does not have access to customer backup data; each customer has their own unique key to access their backup data. This gives not only logical separation from the Druva control plane but also prevents data leakage in the cloud for data at rest.

The customer encryption key is a session-only based key algorithm modeled on digital envelope encryption and results in the customer key never being stored unencrypted, transferred or accessible from outside a user's active cloud-side session. Thus, the need for expensive and complex key management solutions is eliminated.

An additional layer: Deduplication for data at rest

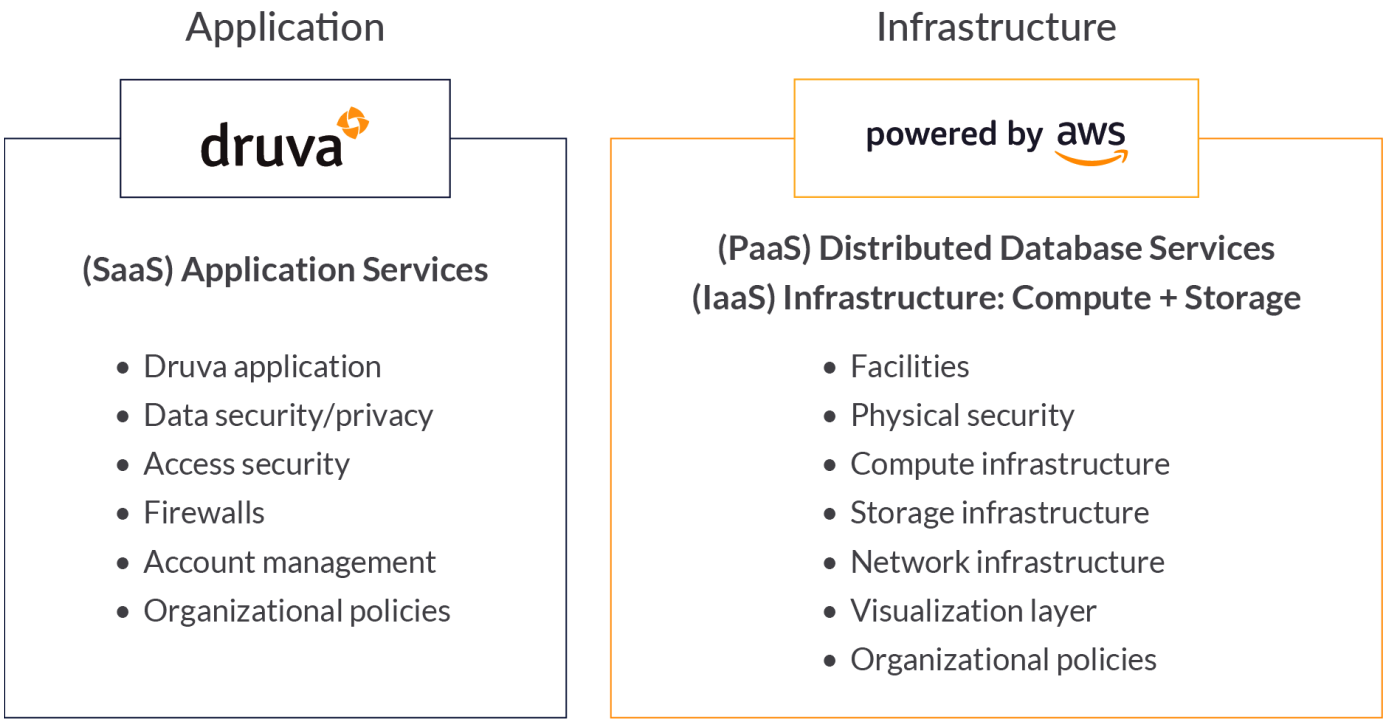
Druva's patented deduplication technology provides another layer of security. Deduplication, or "dedupe," refers to files being separated into individual blocks. Only unique blocks are sent to the Druva Cloud Platform globally, across all devices. This means that entire files don't have to be repeatedly stored and replaced when changes are made—just some of the building blocks.

These unique blocks are stored in object-based storage repository without any identifying metadata, while block reference data and associated source file metadata are stored in a separate object-based NoSQL database. This approach completely obfuscates the underlying data. 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 anyone to decrypt and reassemble the information without authenticated customer credentials.

Shared security for the cloud

Building SaaS applications on top of cloud-based infrastructure requires shared security responsibilities. Druva protects data across the entire stack—from infrastructure to application. The Cloud Service Provider (CSP) provides security for the infrastructure and platform layers, while the software delivers additional security functionality, safeguarding the information residing within the application being hosted.



Data resiliency and storage efficiency

Druva uses AWS S3 which provides a highly durable storage infrastructure designed for mission-critical and primary data storage. Objects are redundantly stored on multiple devices across multiple facilities in an Amazon S3 region. Amazon S3 also regularly verifies the integrity of data stored using checksums. If Amazon S3 detects data corruption, it is repaired using redundant data. In addition, Amazon S3 calculates checksums on all network traffic to detect corruption of data packets when storing or retrieving data.

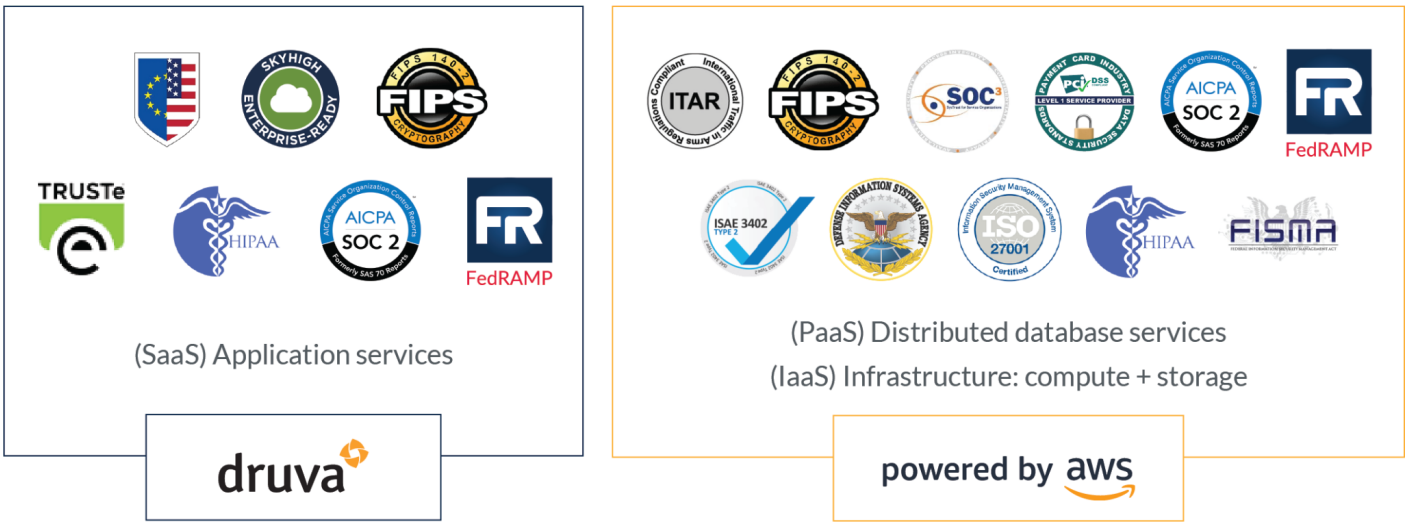
Moreover, Druva internally performs periodic integrity checks to ensure restorability of customers data. This involves simulating a full restore of data. If any of the files are not restorable, subsequent backup ensures that the files are fully backed up again. Druva also stores a checksum of each block which is periodically integrity checked to avoid bit rotting.

Druva goes beyond CSPs for certifications

We're proud of the third-party validation that supports the trustworthiness of our security—one of our core pillars. While many cloud SaaS vendors simply rely on the certifications that the CSPs provide for the infrastructure as their security model, Druva has gone above and beyond, achieving compliance and attestations for our cloud service.

To date, Druva is certified or can claim compliance with the following certifications and frameworks, including (but not limited to):

- SOC 2 type II audited
- HIPAA compliance
- FIPS 140-2 compliant (GovCloud environments)
- FedRAMP moderate ATO (inSync GovCloud environment)



http://security.nknu.edu.tw/crypto/faq/html/2-2-4.html

Single sign-on simplifies access

When the number of applications increases, so does complexity. The addition of SaaS-based applications generates challenges like managing authentication and user access, and effective scaling across a variety of device types and browsers. Organizations have embraced cloud-based, single sign-on (SSO) solutions to handle Identity and Access Management (IAM) holistically. To seamlessly integrate with this strategy, Druva supports the use of cloud-based SSO solutions such as Okta, Ping Identity, and Microsoft ADFS for both administrators and end users. Organizations can also leverage more traditional directory services implementations such as Microsoft Active Directory or LDAP for user authentication, if necessary.

Manageability and traceability keep data audit-ready

Traceability of security events on any device is a standard requirement in any regulated environment. Druva supports the use of audit logging of security events for both users and administrators. Audit logging for Druva's SaaS applications is done in real time, on an event-driven basis, 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.

RBAC affords granular privilege control

In order to prevent privileged users from making unauthorized changes to resources within their own instance of the Druva Cloud Platform, Druva has implemented role-based access control (RBAC). This capability allows organizations to limit privileged user access to a predefined set of roles and data assets, making it possible to create ethical walls to enforce privacy. RBAC also enables the implementation of a delegated administration structure to meet customers' organizational, compliance, and/or security requirements.

Conclusion

As the use of cloud-based SaaS applications continues to grow, so will the need for proper security—and more importantly, information governance capabilities—so organizations have total visibility of their information, no matter where it resides. The good news is we have the tools and the knowledge to deliver security in the virtual environment, improving the state of virtual security over time.

To learn more, visit druva.com/products/enterprise-security

druva Sales: +1 888-248-4976 | sales@druva.com

Americas: +1 888-248-4976
Europe: +44 (0) 20-3750-9440
India: +91 (0) 20 6726-3300
Japan: +81-3-6890-8667
Singapore: +65 3158-4985
Australia: +61 1300-312-729