White paper

Druva Phoenix enterprise-class security

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

Q121-20136

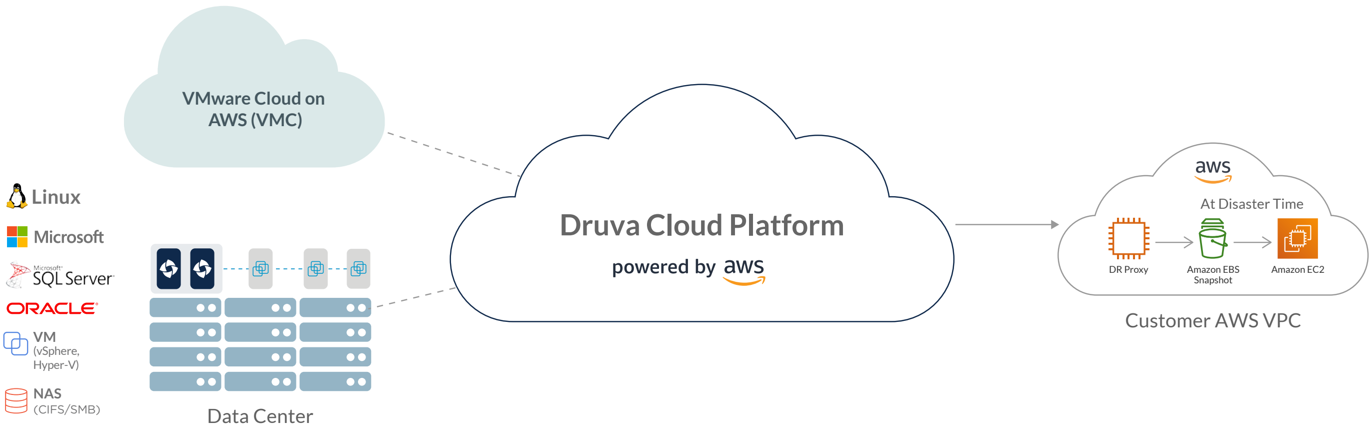
Executive summary

Druva keeps enterprise data 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 security 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.

Druva Phoenix overview

Delivered as-a-service, Druva Phoenix combines high-performance, scalable all-in-one backup, disaster recovery (DR), archival, and analytics to simplify data protection, dramatically reduce costs, and improve data visibility for today's complex information environments.



By leveraging cloud-native technologies, Druva Phoenix removes the traditional bottlenecks of computing and scale, delivering a high-performance cloud platform that enables organizations to replace on-premises solutions and still meet or exceed their RPO and RTO targets.

Druva Cloud Platform overview

The Druva Cloud Platform is a fully-automated, enterprise-class data protection solution powered by Amazon Web Services (AWS) technology. It offers elastic compute and on-demand storage that can grow to accommodate any number of users and data. In addition, the Druva Cloud Platform can be instantly provisioned to a global-user base with policies that lock user storage to specific AWS regions.

The Druva Cloud Platform provides secure, lightning-fast backup and restores and operates in 14+ AWS regions around the world to address the needs of global enterprises. It delivers high availability and is built on an enterprise-class infrastructure that is compliant with international standards such as ISO-27001, SOC-1, SOC-2, and SOC-3.

Additionally, to ensure the utmost security confidence for enterprises, Druva itself has been SOC-2 and HIPAA audited and conducts quarterly vulnerability scans and annual third-party penetration tests.

Full administrative control of Druva Phoenix is provided via a secure, web-based administrator control panel over HTTPS, which allows corporate policies to be defined for servers. Druva Phoenix supports Role-Based Access Control (RBAC) that allows for delegated administration. This enables organizations to implement separation of duties within their specific management domain and without access or visibility into the management domains of other organizations in an enterprise.

On the client side, a lightweight agent manages backup and source-side deduplication. Provisioning is a two-step process that is easily scripted for mass deployment scenarios.

Druva Cloud Platform security

In order to thoroughly 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 Platform 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:

- Logical segmentation of customer records
- Customer data encryption using a unique per tenant AES-256 encryption key

Data in flight

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 Cloud Platform service encrypts data in transit with 256-bit TLS 1.2 encryption by default, 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. A unique AES 256-bit data encryption key is used for each customer account. Druva has implemented an envelope encryption mechanism to encrypt the data encryption key when stored using a customer held key encryption key. The use of one unique encryption key per customer along with customer held key encryption keys, creates crypto-segmentation between customers, completely avoiding data leakage.

Network security

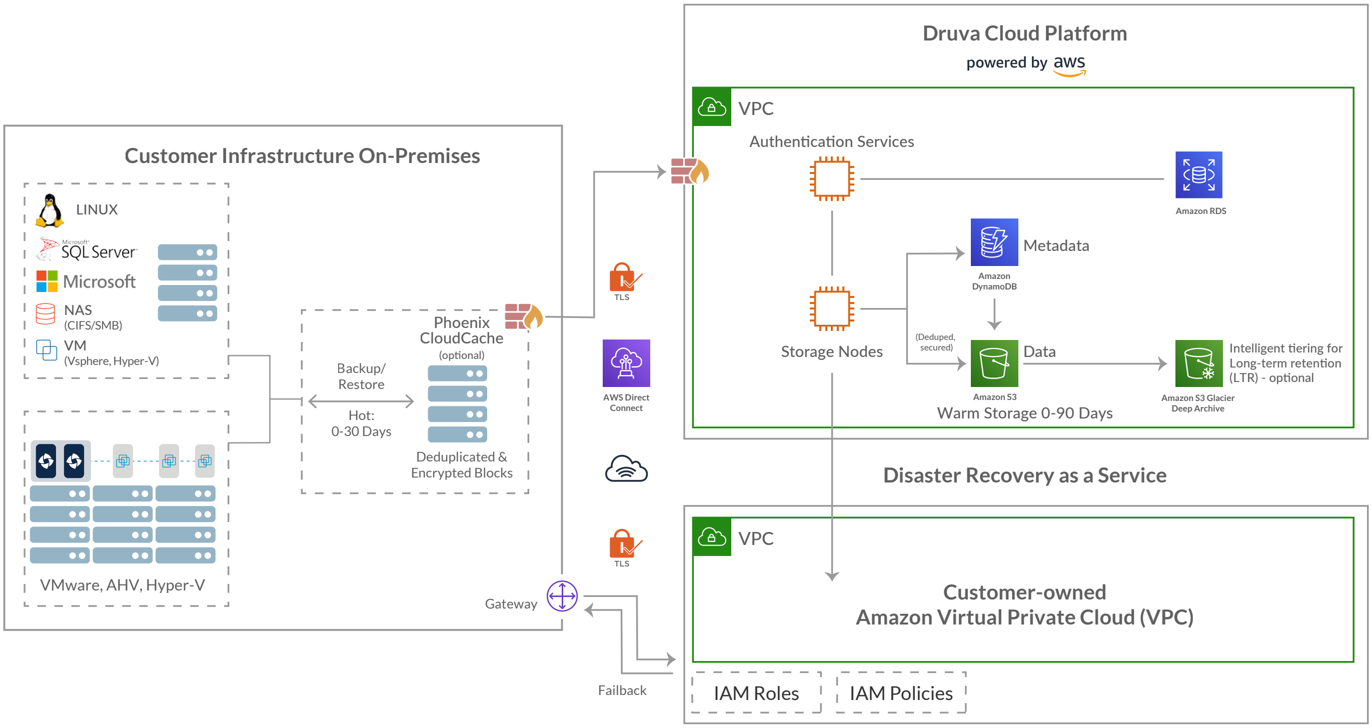
Above and beyond the security mechanism that Druva provides as part of the Druva Phoenix SaaS offering, the AWS network provides significant protection against network security issues, including (but not limited to):

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

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

Druva Phoenix architecture

This diagram shows an overview of the architecture of the Druva Phoenix solution, including its security capabilities:



Druva Phoenix architecture components

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

Amazon Web Services

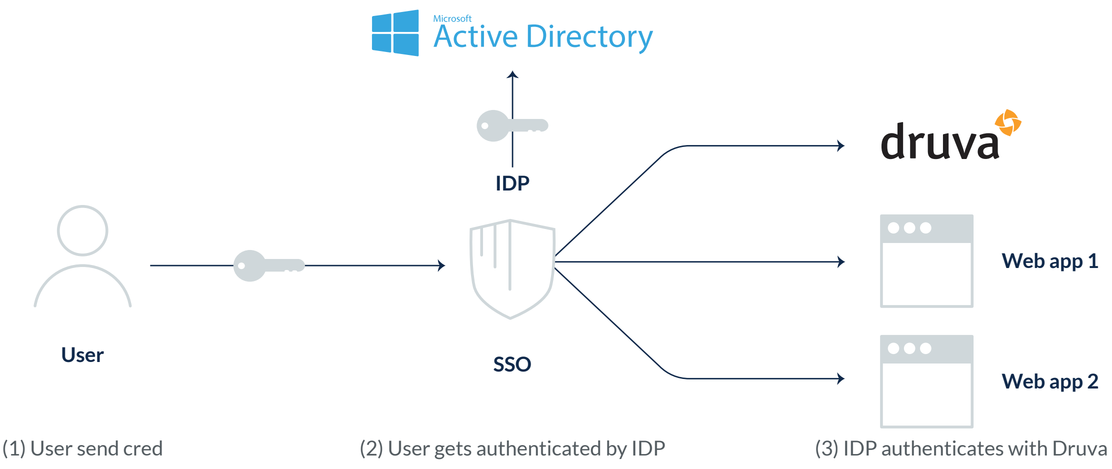
The Druva Cloud Platform, where the Druva Phoenix SaaS application resides, is built on top of the AWS technology stack. Amazon is a world leader in designing, constructing, and operating large-scale data centers throughout the world. The only people who know the actual locations of these centers are those within Amazon with a legitimate business need to have the information. The data centers themselves are secure and meet ISO-27001, SOC-1, SOC-2, and SOC-3 certification requirements.

CloudCache

Druva CloudCache is a local cache designed to help customers meet stringent recovery point objectives (RPOs) and recovery time objectives (RTO) that cannot be met directly by the Druva Cloud. It is delivered as a virtual appliance and stores data from Druva Phoenix agents, then periodically synchronizes this data to the Druva Cloud. It is deployed as a VM on any customer infrastructure on-premises in a data center or other location. If customer bandwidth to AWS is limited or the data set too large to meet RTO from the cloud, CloudCache provides LAN speeds for both backup and recovery operations. CloudCache can deliver scheduled cloud sync to meet tight RTO/RPO needs while allowing customers to control when replication to the Druva cloud occurs. With its flexible scheduling and cache controls, CloudCache retains hot snapshots (up to 30 days) on-premises, while efficiently utilizing your WAN bandwidth to the cloud.

Single sign-on

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


Microsoft Active Directory
IDP
druva
User
SSO
Web app 1
Web app 2
(1) User send cred
(2) User gets authenticated by IDP
(3) IDP authenticates with Druva

IDP: Identity Provider Services (e.g. Okta, OneLogin, Ping One, Azure AD, etc.)

Server agents

Druva Phoenix provides efficient backup of server data directly to the cloud, as well as cloud-based Disaster Recovery (DR) for virtual environments. Effectively protecting server data requires smart integration with multiple structured and unstructured data sources. Druva Phoenix provides the following agents for heterogeneous server environments:

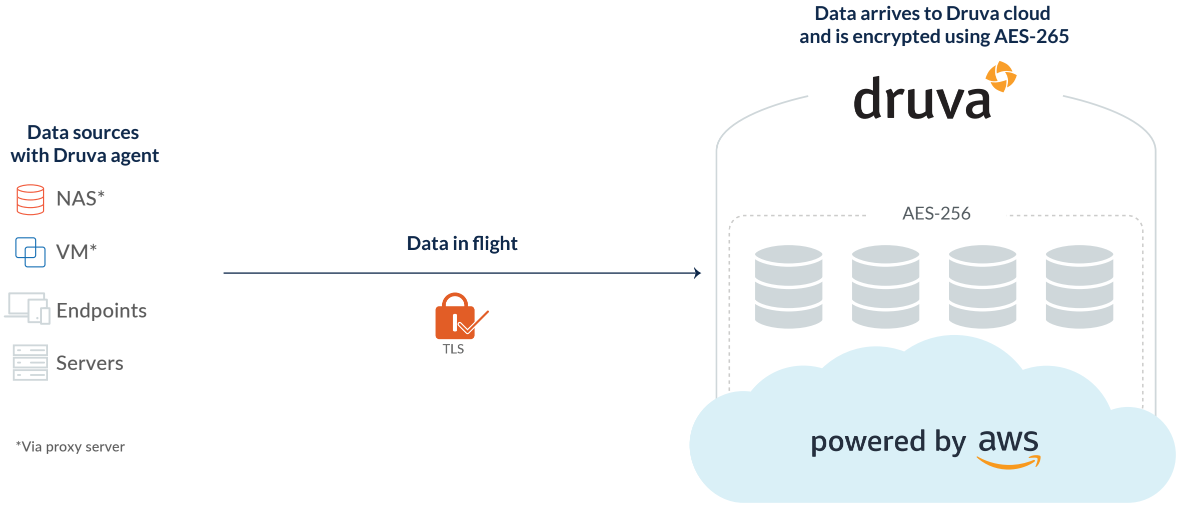
- VMware™ Virtual Machines
- Microsoft™ Hyper-V Virtual Machines
- Microsoft Windows File and Application Servers
- Linux File and Application Servers
- Microsoft SQL Servers
- Oracle Databases
- Network Attached Storage (NAS)

Data encryption

A key attribute of any cloud service is to be able 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 1.2). Data at rest, whether it is stored on-premises with the customer in the Druva Phoenix CloudCache or in the Druva Cloud, is protected with AES-256 encryption. The following is an in-depth look at the Druva Encryption Architecture.

Encryption overview

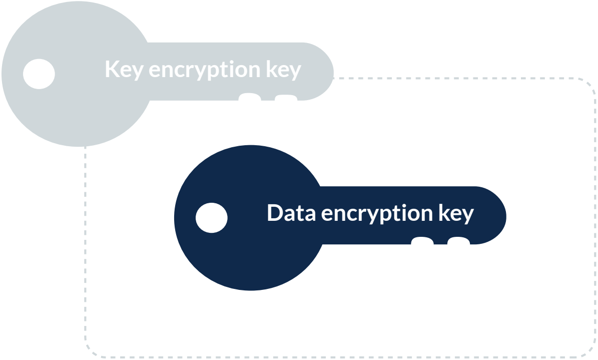
Once the data arrives in the Druva Cloud Platform at the predefined regional storage node over a TLS 1.2 connection, it is immediately encrypted using an AES 256-bit encryption key that is unique to, and completely controlled by, that customer. The following diagram illustrates the encryption flow:



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 only held in memory and never stored unencrypted, 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 Platform is modeled after digital envelope encryption. Digital envelope encryption is the default standard for cloud encryption, and 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 AWS S3. This key is a randomly generated AES 256-bit encryption key that is unique to that individual customer. The DEK is only held unencrypted in memory within the Druva Cloud Platform for use with cryptographic operations I/O operations. At no time is the DEK exposed in plain text form via WebUI or CLI to either the customer or Druva personnel. Additionally, Druva has strict logical access controls to prevent access to production backup nodes. No Druva personnel have direct (SSH) access to servers processing backup operations.

The DEK is generated at the time of the creation of the customer instance in the Druva Cloud Platform 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 a new cloud instance, three things take place:
    a. A randomly generated AES 256-bit encryption is 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, and is 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 Platform. The KEK is generated using a Password-Based Key Derivation Function (PBKDF) by taking the user password or device key, running it through an 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, and is 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, the federal government), we CANNOT do so.
- **Druva CANNOT reset your password.** Because 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, an additional 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—completely obfuscating 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 someone to decrypt and reassemble the information without authenticated customer credentials.

CloudCache encryption

Druva CloudCache is a local cache designed to help customers meet stringent recovery point objectives (RPOs) and recovery time objectives (RTO) that cannot be met directly by the Druva Cloud. It is delivered as a virtual appliance and stores data from Druva Phoenix agents, then periodically synchronizes this data to the Druva Cloud. While this virtual appliance lives on-premises with the customer, the need to secure customer information is just as great as it is in the cloud environment.

Druva CloudCache encrypts data using AES 256-bit encryption. This encryption key is a different Data Encryption Key (DEK) than the key used to store data in the Druva Cloud.

Operational security

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 and follows 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

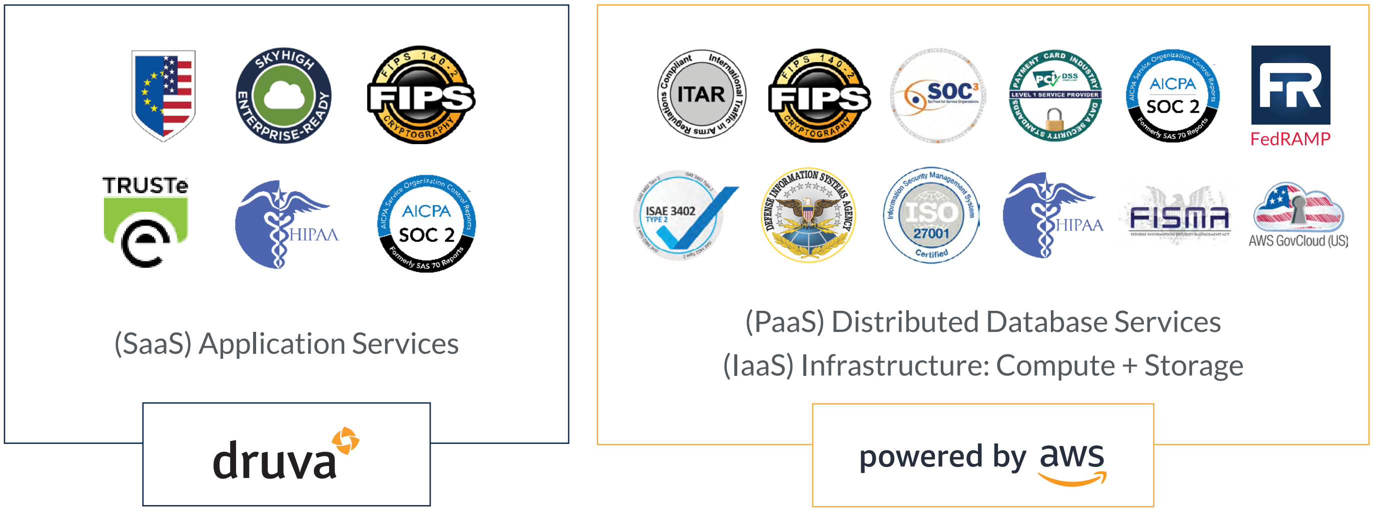
Built-in clusters across a variety of global regions, AWS data centers are designed to anticipate and tolerate failure while maintaining service levels. The Druva Cloud Platform provides multi-zone replication of various elements of customer data including configuration, metadata, and the actual data—thereby ensuring that customer data is accessible from multiple availability zones, to mitigate the failure of any single zone.

Third-party certifications

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)

Phoenix (SaaS) application



(SaaS) Application Services

(PaaS) Distributed Database Services
(IaaS) Infrastructure: Compute + Storage

These certifications are available from Druva upon request.

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

Druva™ delivers data protection and management for the cloud era. Druva Cloud Platform is built on AWS and offered as-a-Service; customers drive down costs by up to 50 percent by freeing themselves from the burden of unnecessary hardware, capacity planning, and software management. Druva is trusted worldwide by over 4,000 companies at the forefront of embracing cloud. Druva is a privately held company headquartered in Sunnyvale, California and is funded by Sequoia Capital, Tenaya Capital, Riverwood Capital, Viking Global Investors, and Nexus Partners. Visit Druva and follow us @druvainc.