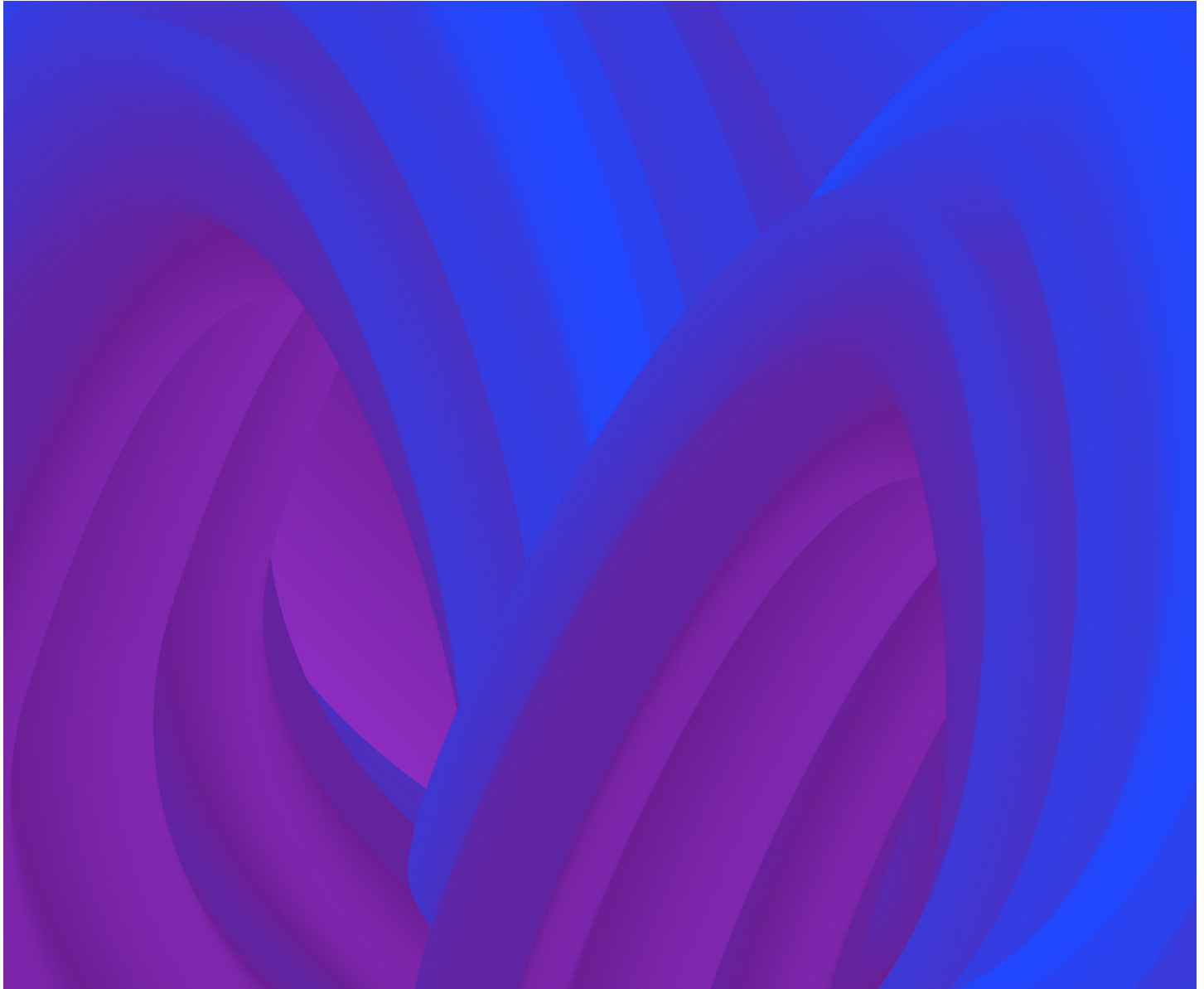




Druva Security Brief: Endpoints and SaaS Applications

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

Executive Summary

Druva bolsters enterprise data defense with the Data Security Cloud, a 100% SaaS, fully managed platform that enhances data protection, monitoring, and recovery. Druva ensures secure and clean recovery through air-gapped, immutable backups, and advanced anomaly detection to facilitate early threat identification.

The platform's integrated response capabilities allow organizations to assess and address threats promptly, and bounce back to clean data without loss. By combining these features, Druva complements existing perimeter defenses, providing a seamless, comprehensive solution that simplifies the response and recovery process and ensures robust protection against modern threats.

This document is designed to provide a quick and convenient review of the security measures Druva has put in place to protect all customer data with a specific focus on solutions for Endpoints and SaaS applications (i.e., M365 or Google Workspace) data.

Druva takes a multifaceted approach to data security that includes data access, data analysis, and advanced encryption.

Druva Endpoint and SaaS Application Data Security Overview

Druva Data Security Cloud simplifies backup, archival, compliance, and device management to reduce the cost and complexity of protecting Endpoint data, support regulatory compliance, and improve data visibility.



* Represents workloads supported at publication date. See www.druva.com - solutions and/or technologies pages for the latest.

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

With enterprise-class security compliant with many international standards including SOC 2, ISO 27001, CSA Star, HIPAA, IRAP, DESC, and FedRAMP/StateRAMP, Druva offers elastic, on-demand storage that can grow to accommodate any number of users and data. In addition, it can be instantly provisioned to a global user base with policies that lock user storage to specific regions.

Druva offers secure, lightning-fast data backups and restores. Operating within multiple storage regions across the world to address the needs of the global enterprise.

Full administrative control of Druva 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 can change settings on their accounts.

On the client side, the Druva agent is a lightweight, non-intrusive client application that manages data backup along with other endpoint services, such as DLP, 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 other devices.

Druva Data Security Cloud Overview

Druva Data Security Cloud is architected on top of secure Amazon Web Services (AWS) infrastructure, and enables air-gapped protection, data immutability, and robust encryption, ensuring foundational security and rapid data recoverability. Smarter and quicker response capabilities allow organizations to assess and address incidents promptly, complementing existing perimeter defenses, to provide accelerated recovery and robust protection against modern threats. Druva's integration with leading OPSEC tools enables organizations to safeguard data across all environments, simultaneously reducing overall risk and operational costs.

Built using Zero Trust Architecture (ZTA) principles, the Druva Data Security Cloud uses separate, air-gapped storage and control planes to enable secure and scalable protection, high availability, and enterprise-scale RPO and RTOs for a wide range of systems including on-premises and virtual infrastructure, cloud workloads, SaaS applications, and endpoints. With elastic compute and on-demand storage, Druva can accommodate any number of users and any amount of data. Storage operations in 20+ AWS regions around the world, and the ability to quickly support new regions, allow Druva to provide secure, lightning-fast backup and restores while addressing the data locality needs of global enterprises.

Additionally, to ensure the utmost security confidence for enterprises, Druva itself has been audited for the above standards and conducts regular vulnerability scanning and annual third-party penetration tests.

Full administrative control of Druva is provided via a secure, web-based administrator control panel over HTTPS, that allows corporate policies to be defined for workloads. Access to the Druva console supports Single Sign-On (SSO), native Multi-Factor Authentication (MFA), and Role-Based Access Control (RBAC) that provides for delegated administration, enabling 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 Managed Data Detection and Response (DDR)

Druva Managed Data Detection and Response (DDR) is a threat detection and response service provided to all customers. As part of the service, Druva actively monitors the security posture of each customer backup environment, sends alerts to notify customers of any potential issues, and assists with the incident response and recovery to accelerate your return to normal operations.

The Managed DDR service includes the following benefits for customers:

- 24x7x365 monitoring of backups for early threat detection
- Expert analysis by Druva Incident Response to provide data insights for any anomalous behavior
- Pre-built response runbooks and automatic lockdown of backups to safeguard data
- Expedited support and expert assistance to customer IR, and backup teams during cyber recovery

Druva Core Security Principles

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 Code Development:

Druva follows security practices throughout all phases of SDLC that are focused on identifying and mitigating risks. Aligning with NIST SP 800-218 Secure Software Development Framework (SSDF) and other industry-recognized standards, Druva's product security program is focused on:

- Building secure software products and platforms which include activities like:
 - Product security requirements
 - Architecture risk analysis and threat modeling
 - Code scanning in CI/CD
 - Internal and external penetration testing
 - Vulnerability management
- Protecting against software supply chain risks
- Secure delivery and support

Digital signatures — All Druva binaries are digitally signed along with the following strategies in place:

- Versioning
- Signature verification

Secure Communication:

- **Unique authentication keys —**
Every proxy and agent has a unique authentication key which is verified in the Druva Data Security Cloud.
- **Encrypted client-server communication —**
All communication to and from the Druva Cloud by devices/agents/proxies is done over TLS v1.2.
- **Encrypted authentication keys —**
The authentication key is encrypted on a device with a device specific encryption key that is generated in combination with unique device information preventing the possibility of this key being spoofed on any other device.
- **Unidirectional communication —**
Agents connect to the Druva cloud, via 2 different URLs utilizing port 443. One URL for receiving backup/restore/upload logs commands, and the other URL is used to fetch or update configuration data to and from the cloud. Both of these connections are initiated by the agent.

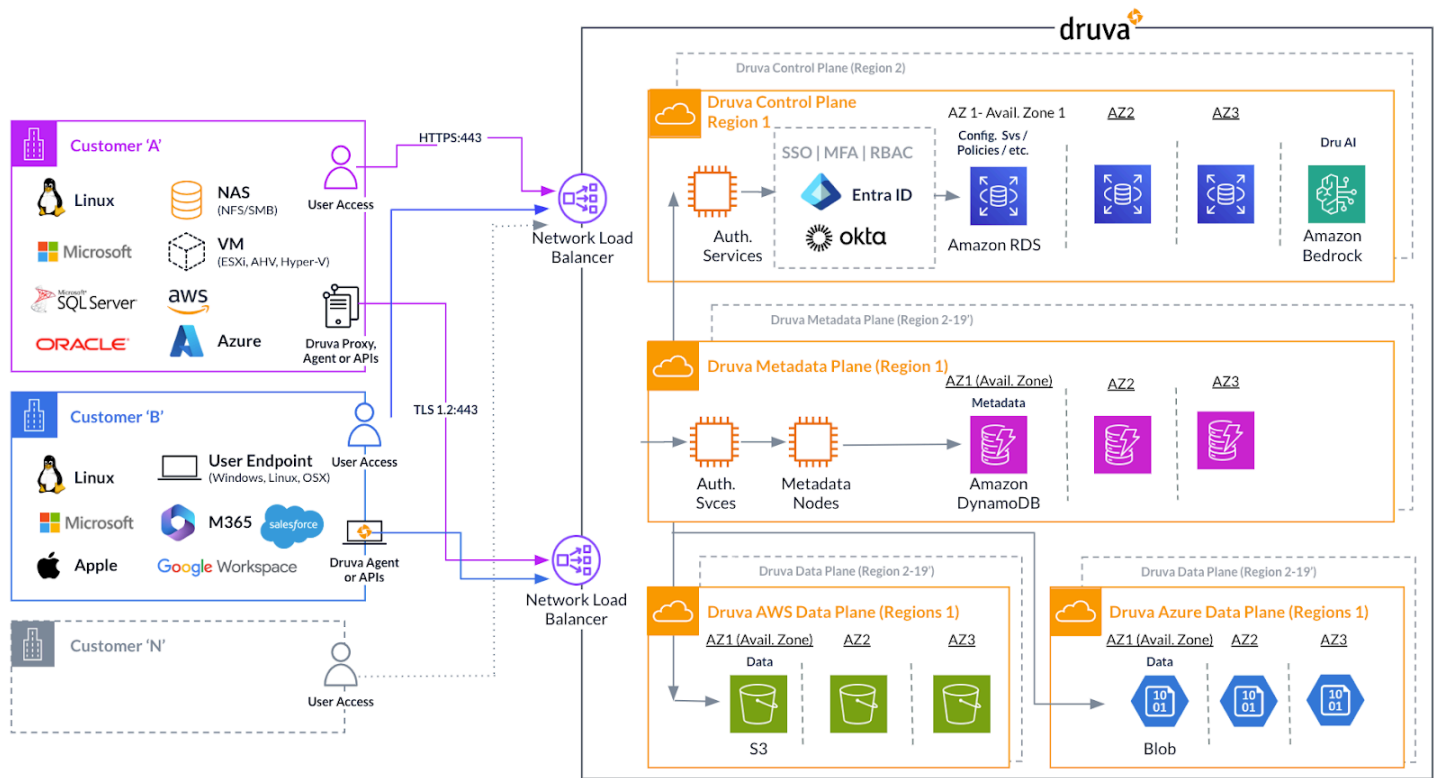
The Druva Data Security Cloud provides a secure, multi-tenant environment for customer data. Each customer's data is stored in its own unlabeled bucket, with each operation performed in a customer-specific context, ensuring complete isolation of all data and metadata into each customer's unique tenant.

This secure multi-tenancy is realized by:

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

Druva Data Security Cloud Architecture

This diagram shows an overview of the architecture of the Druva Data Security Cloud when used for endpoint and SaaS workloads.



* Not inclusive of all workloads supported. See www.druva.com - solutions and/or technologies page for the latest.

Druva is composed of multiple components that, when combined, provide complete protection of customer information. The components are as follows:

Amazon Web Services

The Druva Data Security Cloud is built on top of the AWS technology stack. Amazon is a world leader in designing, constructing, and operating large-scale data centers worldwide. Amazon data centers provide unparalleled physical security with controls at the perimeter layer, infrastructure layer, data layer, and environmental layer.

Network Security

Druva logically separates data and control plane traffic into individual VPCs with segmented public/ internet gateways, non-routable subnets, appropriate deployment of Security Groups, and constant network monitoring and alerting for all of the components supporting the Druva Data Security Cloud. Ensuring Druva architecture aligns with vendor-recommended and Cloud Security best practices around Zero Trust Network Architecture (ZTNA).

Above and beyond the security mechanism that Druva provides as part of the Druva 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/.

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. Druva encrypts data in transit with TLS 1.2 encryption by default.

Data At Rest

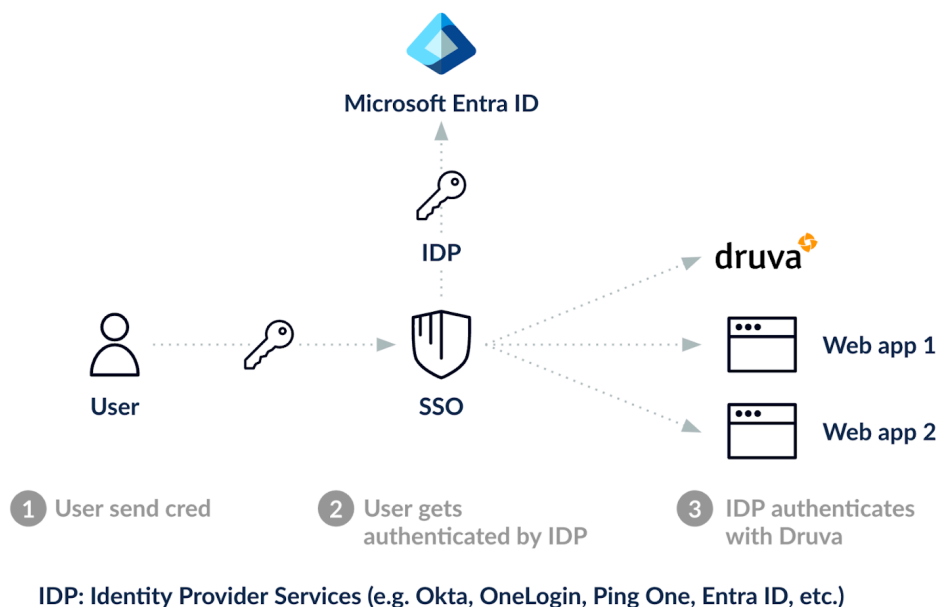
Druva secures data in storage using OFB-AES-256 block ciphers. A unique AES 256-bit data encryption key (eKey) is used for each customer account. Druva has implemented an envelope encryption mechanism to encrypt the eKey when it is stored using a customer-managed encryption key (KEK), which is derived from the customer's password using PBKDF2. The KEK is tokenized and stored in an encrypted database. The use of one unique encryption key per customer, along with customer-held KEK, creates crypto-segmentation between customers, completely avoiding data leakage.

Bring Your Own Key (BYOK)

Enterprise Key Management allows customers to use keys from their AWS KMS account to encrypt and decrypt their data. Customers can host their keys in their own AWS Key Vault. This feature also supports all AWS-integrated third-party enterprise keys like Thales. With this feature, the customer has full control over the data protected by Druva.

Single Sign-On

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



Logging & Auditing

Traceability of access events on any device is a standard requirement in any regulated environment. Druva supports the use of audit logging of access events for both users and administrators, no matter what device they're using. Audit logging for Druva is done in

real-time, on an event-driven basis, and is complete with time and date stamping. Audit logs can be stored on the system based on customer requirements and downloaded for additional analysis in CSV or HTML format.

User Provisioning — Microsoft Active Directory / Entra ID / Google Workspace Integrations

Druva provides integration for the provisioning of users (and administrators) from both Microsoft and Google environments. For Microsoft, the AD connector extends all of the benefits of deep Microsoft Active Directory integration to Druva, enabling integrated mass deployment of the Druva client, automatic user provisioning and de-provisioning, user authentication, and user/ admin management. Similarly, Druva has native user provisioning integration with Entra ID (previously called Azure AD) and Google Directory Services. Customers can choose their own user provisioning method to sync users to Druva.

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.

Operational Security

Druva employees have no access to any of the 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 telemetry 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 Data Security 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.

Remote Wipe

To prevent data breaches on lost or stolen devices, Druva provides remote wipe capabilities across laptops and smart devices that can be executed either by an administrator or 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.

Retention & Version Control

Druva enables its customers to preserve infinite restore points for protected data. Administrative control provides the ability to specify snapshot retention at the backup policy level. If this option is chosen, an automatic process called 'compaction' runs periodically to remove any files that lie outside of the retention rules.

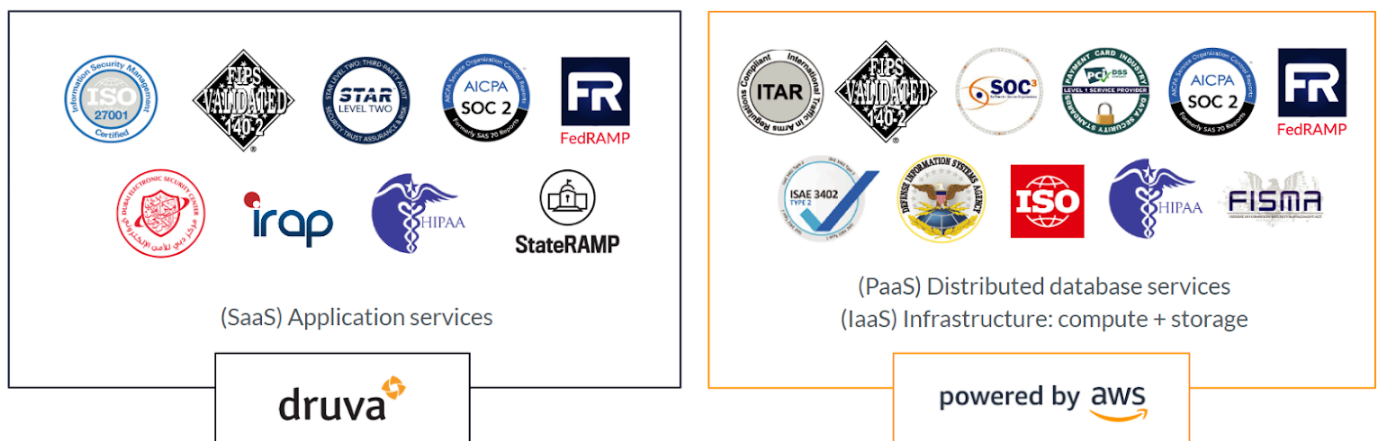
Administrators with appropriate rights also can selectively remove and restore points from individual accounts where required. End users of the system have no control over the removal of stored files, thus keeping the ownership of protected data with the administrator.

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), Druva provides a unified way for IT to quickly assess and take corrective action for non-compliance on regulated or policy-managed, endpoint data.

Secure Discovery & Response

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



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 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 report
- HIPAA compliance
- CSA Level 1 and Level 2 certifications
- ISO 27001:2022
- FIPS 140-2 compliant (GovCloud environments)
- FedRAMP "Moderate" ATO (GovCloud environment)
- Dubai Electronic Security Control (DESC)
- Australian Government IRAP Compliant (Public Cloud)

These certifications are available from Druva using a self-service portal at security.druva.com

druva Sales: +1-800-375-0160 | sales@druva.com

Americas: +1-800-375-0160
Europe: +44 (0) 20-3750-9440
India: +91 (0) 20 6726-3300

Japan: japan-sales@druva.com
Singapore: asean-sales@druva.com
Australia: anz-sales@druva.com

Druva is the leading provider of data security solutions, empowering customers to secure and recover their data from all threats. The Druva Data Security Cloud is a fully managed SaaS solution offering air-gapped and immutable data protection across cloud, on-premises, and edge environments. By centralizing data protection, Druva enhances traditional security measures and enables faster incident response, effective cyber remediation, and robust data governance. Trusted by over 6,000 customers, including 65 of the Fortune 500, Druva safeguards business data in an increasingly interconnected world.