druva



# Security and innovation with Druva FedRAMP cloud

A FedRAMP-certified established data security provider for government agencies, Druva manages a spectrum of SaaS data in the cloud, while enhancing security and mitigating identified risks.

## The challenge

The Federal Risk and Authorization Management Program (FedRAMP) provides a standardized framework for the security assessment and authorization of cloud products and services. With 14 applicable laws and regulations, and 19 standards and guidance documents, FedRAMP certification is the most rigorous security assessment and authorization for cloud products and services.

To put the challenges in context, here is a scenario. A large federal government agency chooses a vendor to migrate their on-premises assets to the cloud. The vendor sub-contracts the management of the migration to a third-party consulting firm. A disgruntled employee with the sub-contractor deletes all of the user data in the cloud environment before leaving the firm. The deletion paralyzes the agency's operations over the next few days and costs them $0.5 million to restore the data. A worst-case scenario would be the data getting exfiltrated to third parties or nation-state bad actors.

Given such risks, as federal government agencies adopt FedRAMP, they need to ensure that their vendors fulfill the three most important evaluation criteria:

1. **Capability assessment:** Your cloud service provider (CSP) should be evaluated against what FedRAMP categorizes as its data security objectives: confidentiality, integrity, and availability. Does the vendor fulfill these requirements not just for their own SaaS applications and platform layers, but also across the infrastructure layer provided by their technology partners?
2. **Cloud service risk evaluation:** Determine the security impact and risk levels of the CSPs against your organization's security objectives. More than 80% of SaaS applications that require FedRAMP certification are moderate impact systems, which is adequate for protecting agencies from any serious adverse effects arising from the loss of confidentiality, integrity, and availability.
3. **Data governance and ownership:** Data that is not publicly available, like personally identifiable information, is considered controlled unclassified information (CUI), which can reside in many places, from data centers to endpoints. The loss or breach of CUI can have serious consequences for agencies, including disrupted operations, lost assets, and exposed personnel files.

Accountability can be difficult when multiple stakeholders get involved in delivering the service. Government customers would want their vendors to take on the responsibility for data governance and complete end-to-end ownership of the data.

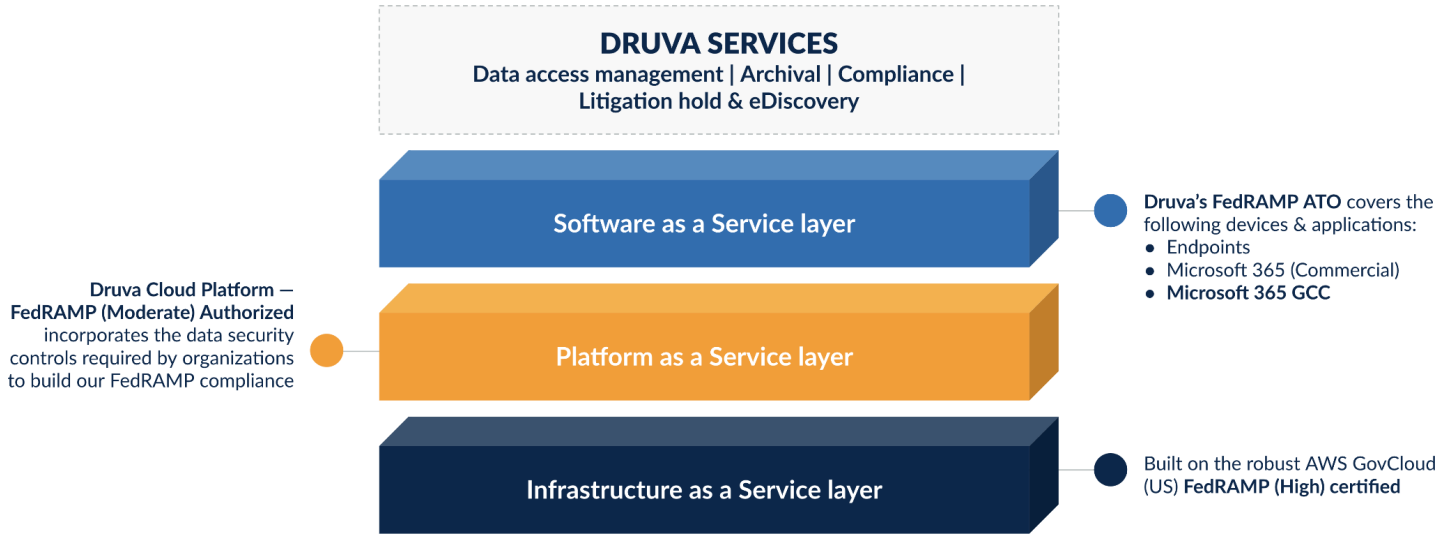
## The solution

**Established vendor trusted by government agencies**: Druva has been supporting hundreds of thousands of end users with its FedRAMP ATO cloud since 2017, establishing a long-lasting first-mover advantage over other industry providers.

Druva, the leading enterprise-class, 100% SaaS data protection vendor with a FedRAMP Moderate ATO certification, serves over forty government agencies including the National Aeronautics and Space Administration (NASA) and the National Institute of Health (NIH).

**FedRAMP certified SaaS ecosystem:** The Druva Data Resiliency Cloud (FedRAMP Moderate ATO), is hosted on the AWS GovCloud, a sovereign cloud dedicated to U.S. government agencies and contractors. AWS is the only cloud infrastructure provider that has the FedRAMP High ATO accreditation today.

## Druva cloud data protection for government agencies




Additionally, Druva also meets several stringent federal regulations and compliance requirements, including FIPS 140-2, Defense Federal Acquisition Regulation Supplement (DFARS) 800-171, and NIST 800-53.

Consistent with our first-mover position in the Federal market, Druva received GCC (High) accreditation in 2021. The Cybersecurity Maturity Model Certification (CMMC), the DoD's certification to standardize the implementation of cybersecurity across the Defense Industrial Base (DIB), is an evolving standard and is currently undergoing reviews and alignment. However, Druva is staying ahead of the curve by working towards a compliant status with CMMC. This underscores Druva's consistent focus on creating a portfolio of highly secure compliance-based cloud services for U.S. government agencies.

Druva offers pre-built integrations with security, identity and user management, IT ops, SaaS ops, and eDiscovery / forensic tools that service the evolving CMMC mandates as part of our readiness program to maintain continuous compliance.

## Integrations to facilitate CMMC controls

**Accountability and ownership:** Druva conforms to U.S. and global security and compliance regulations, which means peace of mind to our customers. As we do not work with any third-party fulfillment vendors, Druva takes complete responsibility for the FedRAMP data governance and ownership mandates.

By deploying Druva's GovCloud backup solution, your organization can backup CUI and other sensitive data, meet regulatory requirements, guarantee reliable security practices, and safely promote the use of cloud solutions.

While doing all this, it is worth highlighting that Druva has no access to government data as it is always encrypted with a session-based encryption key that is unique to, and completely controlled by the customer. Contrast this with the above-mentioned scenario where a third-party contractor could actually have access to government data.

**"We had to become a more automated, nimble, and agile organization, and cloud backup was the technology we wanted to evaluate. The Druva platform aligned with our goals for digital transformation by replacing our efforts with functions that Druva's automated cloud services can do. We can now spend more time on empowering the NCI staff to fulfill the organization's mission."**

— Jeff Shilling, Acting CIO, NCI

## How it works

Druva uses a 100% SaaS, cloud-native architecture to deliver scalable and secure services to archive, discover, and serve government information systems. Key technology strengths include:

- **Cloud-native:** Druva leverages multi-tenant FedRAMP High certified public cloud architecture and micro-services such as Amazon S3, DynamoDB, and Lambda to create a scale-out service without any single point of failure or performance bottleneck.
- **AWS GovCloud:** AWS GovCloud (U.S.) is an insulated AWS region designed specifically for U.S. government agencies and contractors moving sensitive workloads to the cloud. The GovCloud (U.S.) framework adheres to U.S. International Traffic in Arms Regulations (ITAR) and is FedRAMP High accredited.
- **Government-grade encryption:** Druva provides encryption with FIPS 140-2 validated modules.
- **Designed for government scale:** Druva's proven cloud architecture provides limitless scale for global deployments.
- **Address the unique challenges of Microsoft 365 data protection:** For federal agencies using Microsoft 365 and dealing with CUI, backing up the data into MS Azure Cloud could lead to a violation of a key data protection best practice — separating production data from backup data. By backing up Microsoft 365 data into a non-Microsoft cloud, Druva creates separate fault domains to help ensure data resiliency and redundancy.
- **No hardware:** Druva requires no new hardware. Simply configure your environment and have global reach and scale at your fingertips in minutes, while remaining continuously compliant through any moves, adds, and changes.
- **WAN-optimized:** Data being transferred to and from the cloud is optimized for low latency networks. Druva also offers smart bandwidth throttling, which limits bandwidth consumed for each schedule depending on total available bandwidth.
- **Forever incremental backups with global dedupe:** Data transmitted is deduplicated globally across data present at all sites, making backups truly immutable.

Backups are also incremental forever, which significantly reduces the amount of bandwidth needed to transmit backup data, resulting in considerable cost savings for agencies and customers.

- **Automated storage tiering:** Data retained longer than 90 days is automatically moved to cold storage (AWS Glacier), keeping versioning and dedupe intact.
- **Optional on-site caching:** Data can be cached locally for up to 30 days for faster RTO (Recovery Time Objective).
- **Central visibility and audit:** Druva gives you a comprehensive, single point to view your data protection status, and to manage your data protection services across your environment with ease.
- **Platform independence:** Using the same platform for production and backup data carries the risk that backup data could be unavailable if the platform suffers a global outage. For customers using Microsoft 365, Druva hosts backups on AWS, offering a different platform for backup data.

## Future-proofing against evolving compliance

- **Customized cloud-native solution certified to protect government data anywhere it resides**
- **Druva supports 3-2-1 backup policy with cloud-based data protection**
- **Robust, zero-trust security through data isolation and air-gapped storage**
- **Platform supported by U.S. persons and compliant with requirements of individual government agencies**
- **Druva utilizes AWS GovCloud, the government's most widely accepted cloud platform**

## For more information

To learn more about how Druva is responding to the new Cybersecurity Maturity Model Certification and other government security projects, visit the Druva enterprise data security page.

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

Druva is the industry's leading SaaS platform for data resiliency, and the only vendor to ensure data protection across the most common data risks backed by a $10 million guarantee. Druva's innovative approach to backup and recovery has transformed how data is secured, protected and utilized by thousands of enterprises. The Druva Data Resiliency Cloud eliminates the need for costly hardware, software, and services through a simple, and agile cloud-native architecture that delivers unmatched security, availability and scale. Visit druva.com and follow us on LinkedIn, Twitter, and Facebook.