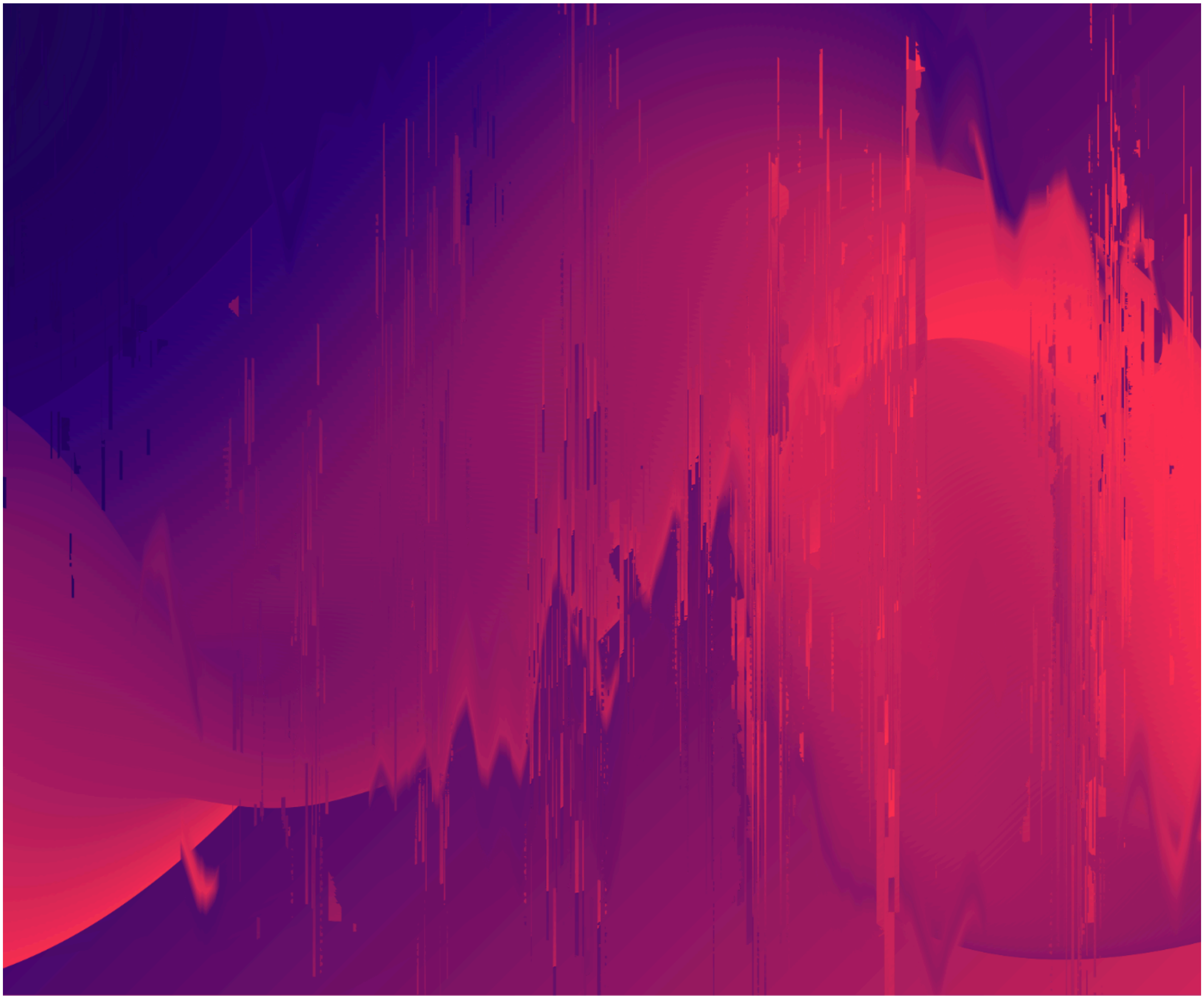
White paper



# Protect. Respond. Recover.

Your blueprint for making data resilient to cyber attacks

## Introduction

Cyber attacks are a continuous threat. You know that. We know that. Wouldn't it be great if there was a simple blueprint for making data resilient and making cyber attacks less scary? Druva is here to help. Here's a three-step process you can use to build your own ransomware playbook. Plus, Druva is here to help every step of the way — our Cloud Ops team is always monitoring the environment and ready to alert, investigate, and initiate restores *for you* in the event of an emergency.

## Step 1: Protect

The first step in being ready for a cyber attack is ensuring a clean, safe copy of your critical data exists. After all, backups do no good if they are encrypted by ransomware. What needs to be done to ensure you always have a clean copy of the data to restore?

### Ensure data integrity and availability

The first line of defense when protecting backup data is to make sure attackers do not have access to where the data is stored. To do this, you need to store immutable copies of backup data on an air-gapped system, protected by strong access controls and security protocols.

#### Protect data with an air gap

Ensuring your backup data is stored on an air-gapped platform is an essential step in protecting your data. An air-gapped platform is one without a persistent connection to your business network, this puts a barrier between critical backup data and other computing platforms.

Ransomware requires a persistent network connection to reach the command and control servers that guide ransomware execution, so air-gapping is critical to data protection success.

#### Use access controls with strong security protocols

Of course, an air-gapped environment is not enough to secure against all threats. Access control is another vital element in data protection. Access to data is necessary for a business to function. Administrators need access to manage the system, and you may want to allow vendors or other applications to access the backup data as well.

However, it's important to ensure that only a select few individuals have administrative access that would make it possible to change or delete backup data. Implementing best practices such as RBAC to limit access to critical backup operations, MFA (Multi-Factor Authentication), and SSO (Single Sign-On) to shore up access security are table stakes when building an environment that ensures data integrity.

#### Make your data immutable

Ensuring your most critical data is immutable can also prevent problems with data integrity. In addition to encrypting data in motion and at rest, your backup solution should give you the option to mark specific data sets as immutable. These data sets cannot be changed, even using administrative credentials.

#### Druva protects your critical data

Druva protects your critical data. It ensures data integrity and availability with air-gapped, immutable backups. There is no persistent network connection to the Druva cloud, and the platform operates without hardware or an operating system. Without access to a persistent network connection or OS, malware cannot execute in the Druva backup environment.

Additionally, data is encrypted in flight and at rest using dual envelope encryption technology. Unique AES-256 encryption keys are issued per tenant. It is impossible for anyone besides the customer — even Druva — to access the data.

#### Security on autopilot — Druva's Managed Data Detection and Response for backups

The concept of MDR, or Managed Detection and Response, has long been offered by security providers as a comprehensive service combining monitoring and threat detection features to enhance an organization's security posture. **Druva is proud to introduce Managed Data Detection and Response for the backup environment**, among the first services of its kind, and included in customer licenses at no additional cost — no third party needed. We have honed our ability to detect early signs of threats through backup telemetry and developed swift response and recovery strategies. Our team of analysts serves as an extra set of eyes on customer data, thoroughly examining generated alerts, and conducting a detailed analysis to rule out false positives. Druva support then communicates with customers, and once the threat has been verified, takes proactive measures to secure and, if necessary, roll back compromised data for them.

### Data lock feature:

It's important to mark critical data "immutable," but existing solutions introduce either security or governance problems. Druva takes a unique SaaS-based approach that solves both security and governance issues.

- **Some competitors offer a "soft lock."** This introduces security issues because it can be undone by a customer admin.
- **Others offer a "hard lock."** This causes governance issues because it cannot be undone, even if data must be deleted for legitimate compliance reasons.
- **Druva's Data Lock** solves both of these issues. The "lock" can only be undone by the Druva support team. Data is secured against malicious access, but can still be deleted if needed for compliance reasons.

With an inherent air gap, truly secure Data Lock, zero-trust security, and automatic patching, Druva's cloud-first SaaS approach to protecting your data lays the foundation for cyber resilience. The next step is to operationalize cyber resilience.

## Operational security

You've chosen a backup solution that can ensure data integrity and availability. Now you need to keep ahead of the attackers. But this isn't as easy as it sounds.

Keeping up with security best practices like vulnerability scans, patching, and upgrades is an ongoing struggle. And attackers know this. Many times the first thing ransomware targets is the backup systems.

If you miss just one update, savvy cybercriminals can execute a successful attack. And you wouldn't be alone; 42% of vulnerabilities are exploited after a patch has already been released but not yet applied by IT personnel.

A SaaS platform is the optimal choice for operationalizing your security efforts. When you choose a 100% SaaS vendor, you can rely on them to manage the hardware, software, and all of the extra processes required to keep ahead of attackers.

### All SaaS, fully managed, always secure

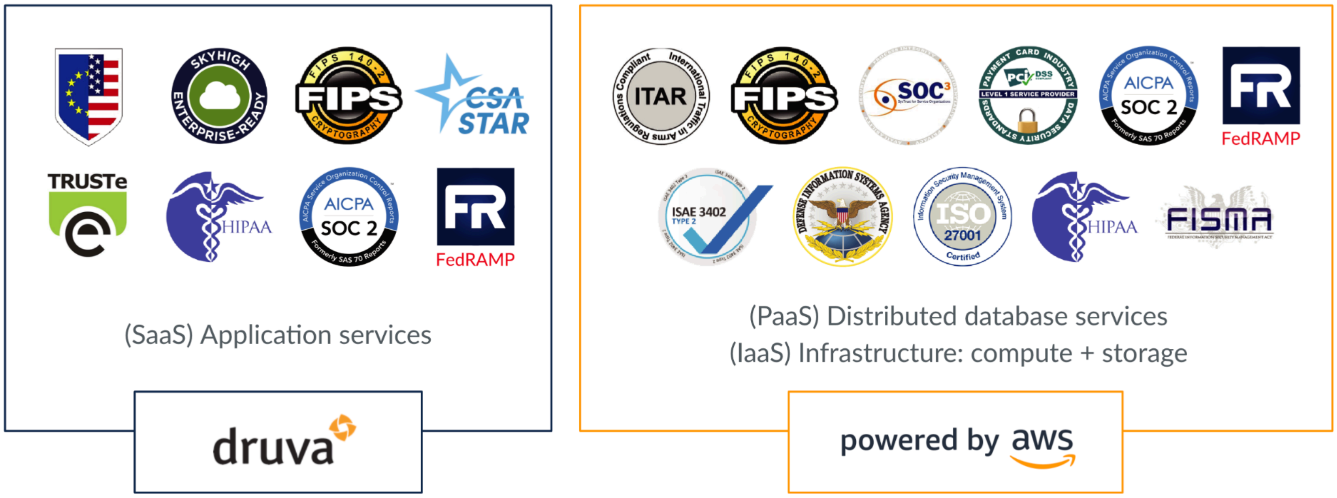
Druva regularly and automatically updates the platform with security patches for you. Never worry about vulnerabilities and rest easy knowing you can recover clean data at a moment's notice.

### Druva's stringent security compliance and 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)

These certifications are available from Druva upon request. In addition to these certifications, Druva has an open Vulnerability Disclosure Policy and has ongoing penetration tests conducted for any security vulnerabilities by third parties (Coalfire, Bishop Fox, Cobalt.io ) to ensure the highest levels of security compliance.



## Step 2: Respond

Now that you are sure your data is safe, you still need to prepare for attacks. Protecting the data is not enough. To be ready to respond in the event of an attack, you must improve your security posture and be proactive to detect problems before they can cause damage.

### Posture and observability

Secure backups and a recovery plan are no longer enough to withstand cyber attacks. You must evaluate and improve your data security posture and ensure you have clear visibility into data wherever it resides. There is a wealth of information in your backup environment that can help you be more prepared. With this information, you are able to correlate data points to paint a full picture of threat vectors, scope, and impact, allowing you to quickly respond to an attack, reduce the impact, remediate for full recovery, and harden your security posture.

> **Observability** is the ability to measure the internal states of a system by examining its outputs, such as logs, metrics, etc. (e.g., you need to be able to know that your backups are functioning well and securely). Observability and monitoring can be used together, but they are not the same thing.

**Here are some ways visibility into your backup environment can help you prepare for cyber attacks:**

#### Security posture

Security posture is a measure of your overall cybersecurity strength and how well you can predict, prevent, and respond to ever-changing cyber threats. There are many primary environment security posture management tools, but most do not address security posture in the backup environment. With attackers targeting backups, it is necessary to ensure parity across your secondary environment.

#### Data anomalies

Ransomware attacks produce anomalies at the data level. The ability to quickly identify anomalous activities or data sets can help you choose a course of action *during* the recovery process and even support the detection of ransomware attacks.

For example, when ransomware attacks the backup system first, the sudden deletion or encryption of data may be a strong indicator of an attack. Wouldn't it be great to be automatically alerted to that activity?

### Malicious access attempts

Situational awareness of activity in your backup environment can help you identify malicious actions such as unauthorized access or deletions. Observing actions taken by users or APIs both before and during an attack can provide important insights.

To take advantage of this observational data, be sure to investigate:

- Which users and APIs accessed your backup environment
- Where access attempts originated geographically
- When access attempts were made
- What actions were attempted (encrypt, delete, etc.)

Observing who (and what) is trying to access your backup data, and what they tried to do, helps illuminate the path to resolving the incident. The ability to use API integrations to feed this observability information from the backup environment into your SIEM (security information and event management) applications like Splunk and ArcSight can accelerate incident response.

### Continuous monitoring

It is critical to continually monitor your backup environment for threats.

> **Because cyber threats like malicious insiders, accidental deletion, and credential compromise are so common, it's important to be able to get data back, even if it was deleted using "authorized" admin credentials.** The Druva Rollback Actions feature stores data in an inaccessible cache for more than seven days, giving you a self-serve way to get your data back, even if it's deleted.

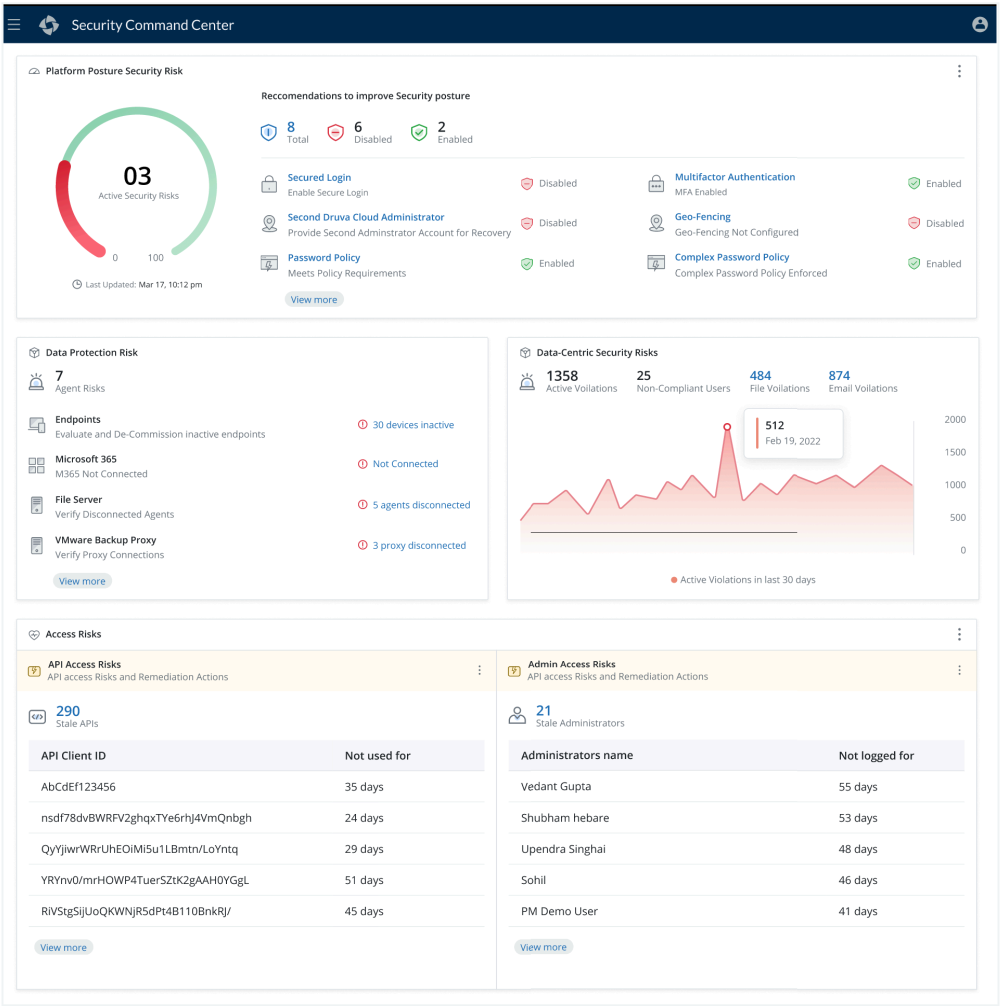
### Full data visibility and Threat Hunting with Druva

To be attack-ready, you must be able to protect your data, prepare for threats, and respond and recover quickly. Druva provides complete visibility into backup security posture, data anomalies, and access attempts in a security center dashboard, powered by unique global data intelligence. In addition, customers get access to **Threat Hunting** capabilities that strengthen their incident response by:

- Searching for threats across an extended timeline of backups and the entire end-user data — endpoint devices and apps like Microsoft 365 and Google Workspace.
- Locating and quarantining threats to prevent restore of compromised data and eliminate reinfection risks.
- Destroying threats from backups and primary environments with defensible deletion.

Druva's security dashboard provides real-time recommendations to help you protect your backups. With it, you can:

- Receive customized suggestions to improve security posture based on your unique deployment.
- Identify and respond to threats with machine learning-based anomaly detection that understands your data and sends alerts for suspicious anomalies.
- Uncover potentially malicious access attempts with clear insight into who or what is trying to access and affect your data.
- Recover data using the "rollback actions" feature, even if it was deleted using "authorized" administrative credentials.
- Facilitate closer collaboration between InfoSec and IT teams to support monitoring, incident response, and root cause analysis through integrations with SIEM and SOAR platforms like Splunk.



Security Command Center

Platform Posture Security Risk

03
Active Security Risks

Last Updated: Mar 17, 10:12 pm

Reccomendations to improve Security posture

8 Total | 6 Disabled | 2 Enabled

| | | | |
|---|---|---|---|
| Secured Login<br>Enable Secure Login | Disabled | Multifactor Authentication<br>MFA Enabled | Enabled |
| Second Druva Cloud Administrator<br>Provide Second Adminstrator Account for Recovery | Disabled | Geo-Fencing<br>Geo-Fencing Not Configured | Disabled |
| Password Policy<br>Meets Policy Requirements | Enabled | Complex Password Policy<br>Complex Password Policy Enforced | Enabled |

View more

Data Protection Risk

7
Agent Risks

| | |
|---|---|
| Endpoints<br>Evaluate and De-Commission inactive endpoints | 30 devices inactive |
| Microsoft 365<br>M365 Not Connected | Not Connected |
| File Server<br>Verify Disconnected Agents | 5 agents disconnected |
| VMware Backup Proxy<br>Verify Proxy Connections | 3 proxy disconnected |

View more

Data-Centric Security Risks

1358 Active Voilations | 25 Non-Compliant Users | 484 File Voilations | 874 Email Voilations

Access Risks

API Access Risks
API access Risks and Remediation Actions

290
Stale APIs

| API Client ID | Not used for |
|---|---|
| AbCdEf123456 | 35 days |
| nsdf78dvBWRFV2ghqxTYe6rhJ4VmQnbgh | 24 days |
| QyYjiwrWRrUhEOiMi5u1LBmtn/LoYntq | 29 days |
| YRYnv0/mrHOWP4TuerSZtK2gAAH0YGgL | 51 days |
| RiVStgSijUoQKWNjR5dPt4B110BnkRJ/ | 45 days |

View more

Admin Access Risks
API access Risks and Remediation Actions

21
Stale Administrators

| Administrators name | Not logged for |
|---|---|
| Vedant Gupta | 55 days |
| Shubham hebare | 53 days |
| Upendra Singhai | 48 days |
| Sohil | 46 days |
| PM Demo User | 41 days |

View more

## Step 3: Recovery

Ransomware attacks are often far-reaching and affect more than one type of data or system. After an enterprise-wide ransomware attack, the challenge is to recover data across all users and workloads as quickly as possible.

Traditionally, recovery looked something like this:

1. The security team determines when the attack started and the scope of impact.
2. Data is restored from a point in time prior to the initial infection.
3. If RPO is too far back, IT teams manually search for more recent, clean versions of data and files.

It's a lot of manual labor that still rarely restores complete data.

This doesn't even take into account issues with reinfection. Restoring contaminated data is every IT administrator's worst nightmare because it takes the recovery process back to square one. That's why it's vital to ensure data is free of malware and other IOCs (indicators of compromise) *before* recovery.

All of these challenges can be addressed with Druva's cloud-native infrastructure and automated recovery workflows.

### Accelerated recovery

Druva provides Accelerated Ransomware Recovery to help you **automate** the process of quickly and cleanly recovering from a ransomware attack. Druva Curated Recovery helps lessen the impact of a ransomware attack by building an uncorrupted recovery point that includes the most recent, unencrypted version of files and data from the entire time frame of an attack. This eliminates the data loss and manual effort rooted in traditional recovery.

What does automated recovery look like?

1. **Using anomaly detection to detect threats early**

   Access Insights give admins a way to understand the location and identity of all access attempts, helping to uncover malicious access attempts associated with the attack.

   Anomaly Detection provides data-level insights on file changes, creation, recovery, and deletion, helping identify the timeframe of an attack.

   Druva can also be integrated with SIEM and SOAR tools for better security orchestration.

2. **Quarantining infected backup snapshots**

   It is critical to quarantine any infected snapshots and stop backups from potentially infected resources to prevent restoring infected data and starting the entire process over again.

3. **Finding the last-known-good version of files**

   Druva Curated Recovery alleviates the manual process of finding the last clean version of a file. The algorithm looks at the history of all the files within the defined time period and then stitches together a single known good recovery point.

4. **Ensuring you don't reinfect yourself**

   With the Recovery Scans feature, the algorithm filters out malicious files that match an AV scan or customer-provided IOCs.

**Security and IT teams need to work together.** Druva makes that easy by exposing data from backup environments as well as rich security logs so security teams can use them for forensics.

## Conclusion

Cyber attacks can cost a business everything from critical data loss and downtime to reputation. You need a blueprint that makes your data resilient so you can protect, prepare, and recover when attacks inevitably occur.

These challenges are often too great to face alone. Druva is the only 100% SaaS data security solution that provides true end-to-end cyber resilience.

Take a tour of Druva's ransomware recovery and security posture solutions, or set up a 30-day trial of Druva to try it for yourself — absolutely free with no credit card info required!

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, the autonomous data security company, puts data security on autopilot with a 100% SaaS, fully managed platform to secure and recover data from all threats. The Druva Data Security Cloud ensures the availability, confidentiality, and fidelity of data, and provides customers with autonomous protection, rapid incident response, and guaranteed data recovery. The company is trusted by its more than 6,000 customers, including 65 of the Fortune 500, to defend business data in today's ever-connected world. Amidst a rapidly evolving security landscape, Druva offers a $10 million Data Resiliency Guarantee ensuring customer data is protected and secure against every cyber threat. Visit druva.com and follow us on LinkedIn, Twitter, and Facebook.