

Druva Data Security Cloud Overview

Data Security on Autopilot for the Modern Enterprise

Modern Enterprises Need Data Security

Over the past decade, data risks have diversified, shifting data protection's role from a passive last line of defense to an active data partner in responding to and recovering from diverse data risks. Traditionally, backup solutions aimed to secure against system risks such as hardware and application failures. However, with cloud making infrastructure redundant and applications becoming more resilient, risks have shifted from infrastructure to the data layer.

Four main data threats have emerged: availability, user, cyber, and process risks. Availability risks, such as those to hardware/applications, require attention to prevent data loss. User threats like malicious exfiltration have become more serious, especially with the rise of AI, which increase the utility and exposure of stolen data. Cyber threats like ransomware continue to pose significant risks, making secure backups essential. Finally, governance and compliance processes have grown with new regulations demanding verifiable accuracy and responsible data handling across the entire lifecycle.

Security tools such as Splunk and CrowdStrike play a critical role in creating defensive layers to secure the enterprise perimeter. However, some threats inevitably breach these defenses. Legacy backup approaches typically resorted to brute force recovery, but modern incident response demands a thorough analysis of the breach's scope, impact, and remediation strategies before recovery can occur. Data security is essential in this process, providing deep data insights that, when combined with perimeter security data, drive comprehensive and effective data-powered incident response.

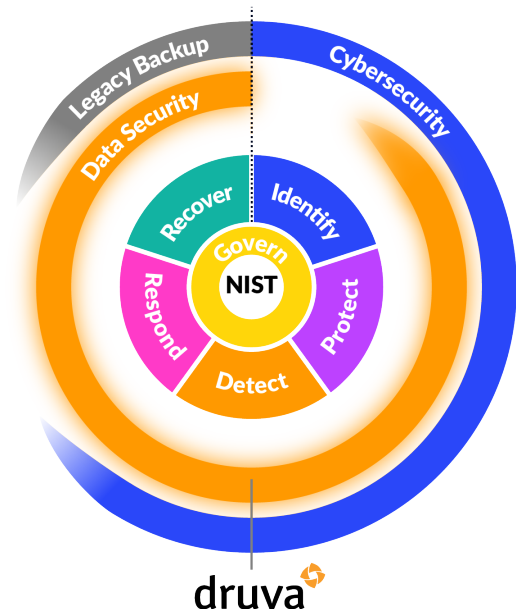
Druva bolsters enterprise data defense with the Data Security Cloud, a 100% SaaS, fully-managed platform that enhances protection, monitoring, and recovery. Druva ensures secure and clean recovery through air-gapped immutable backups, and advanced anomaly detection facilitates early threat identification.

Business challenges

- Accelerate cyber response and recovery
- Secure multi-cloud deployments
- Reduce IT costs and complexity
- Enable AI initiatives
- Protect and secure hybrid workforce

Key benefits

- Fully-managed, 100% SaaS, no hardware or software, secure-by-design; data-powered incident response and recovery
- Automated reinfection avoidance and sandbox recovery to validate clean data and prevent reinfection
- Managed Data Detection and Response (MDDR) included to automate recovery, minimizing data loss and downtime
- Patented AI-driven data anomalies detection and threat hunting
- Unified, simplified management across all workloads — SaaS apps, end-user devices, hybrid workloads, and multi-cloud
- Compliant with the industry's highest standards, including SOC2 type II, HIPAA, FIPS 140-2, and FedRAMP ATO
- TCO savings of up to 40% vs. competing legacy on-premises solutions
- Industry's first and only \$10 million Data Resiliency Guarantee



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.

Druva — Data Security on Autopilot

The Druva Data Security Cloud secures and recovers data from all threats, with the simplicity and speed that only true 100% SaaS can deliver.

Key Capabilities

- **Data Protection** — Modernize backup and restore, disaster recovery, and archive with Druva's air-gapped and immutable platform. Detect threats earlier with integrated, continuous monitoring of the backup and production environments for unusual activity — automate alerts to the SIEM to accelerate response. Unify the security, backup, management, and recovery of all critical data — across SaaS apps including Microsoft (M365, Entra ID, Azure VM), Salesforce, and Google Workspace, as well as endpoints, cloud workloads, hybrid workloads, and more — from one simple console.
- **Cyber Response & Recovery** — Druva provides uninterrupted access to logs, changed data, clean backups, malware scans, and threat hunting, enabling the Incident Response team to assess and contain threats effectively. Quarantine infected backups and delete malware to prevent reinfection. During recovery, ensure clean backups with automated malware scans and sandbox recovery to test data hygiene. Curated Recovery prevents data loss by synthesizing multiple backups to find the most recent clean data, allowing IT teams to restore systems safely and promptly.
- **eDiscovery & Compliance** — Simplify data governance, enhance visibility, standardize policy enforcement, and mitigate risks. Druva enables organizations to monitor, track, and notify users of compliance risks, manage legal holds, and reduce the time and cost of eDiscovery requests. The centralized dashboard provides a federated view of sensitive data, enabling quick access and tracking of compliance violations. Key features include customizable compliance templates, tamper-proof audit trails, thresholds for sensitive data, and the ability to quarantine violations.
- **Platform** — Druva uses a single powerful platform to protect all customer workloads, creating a common metadata namespace for each customer. This enables advanced insights into the lateral movement of threats through the system by piecing together an informed view of the gestation, timeline, and impact across the customers' data. This also unlocks the power of GenAI to enable capabilities such as conversational threat hunting and threat modeling. Additionally, Druva's AI co-pilot, Dru, is always available to assist, troubleshoot, and optimize the solution to enable the best security with the least effort.
- **Fully Managed** — Druva does it all for the customer, removing the complexities of legacy "do-it-yourself" data security. As a 100% SaaS platform, Druva deploys in as little as 5 minutes and does not require the customer to manage any infrastructure or update software — as a result, customers typically see savings of up to 40% vs. competing solutions. Additionally, Druva's Managed Data Detection and Response (DDR) service, included at no extra cost, utilizes backup telemetry to detect threats and offer swift response and recovery strategies with analysts providing proactive measures to secure and roll back compromised data for the customer.
- **Intelligence** — Druva is trusted by over 6,000 customers and growing. As a SaaS platform, Druva continuously analyzes and tracks metadata across this growing install base. When a new cyber incident or threat pattern is detected for one customer, the platform quickly learns from this incident and applies the learnings across the full customer base, regardless of size or industry.

Druva offers a cutting-edge data security solution by seamlessly merging a fully managed platform with a GenAI-powered and unified data namespace. This innovative approach ensures the availability, confidentiality, and fidelity of data, empowering businesses to prioritize and defend against the most critical risks with confidence.

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. Visit druva.com and follow us on [LinkedIn](#), [Twitter](#), and [Facebook](#).



Enterprise Data Security for Microsoft Entra ID

As the backbone of identity and access management (IAM) for Microsoft Cloud resources, Entra ID (formerly Azure Active Directory) is crucial for maintaining business continuity. Druva's 100% SaaS solution provides an efficient, automated, and simplistic way to protect and recover Microsoft Entra ID objects, ensuring your organization remains resilient against disruptions.

The challenge

Microsoft Entra data shows attempted password attacks increased more than tenfold in 2023, from around 3 billion per month to over 30 billion. This translates to an average of 4,000 attempted attacks per second targeting Microsoft Cloud identities¹. If Entra ID isn't available, your users can't work in Microsoft 365 or Azure Cloud. To ensure resilience against Entra ID outages, compromises, and misconfigurations, your organization must have reliable access to its data.

Druva's Microsoft Entra ID solution enables organizations to take a policy-driven approach to protect their Azure Identity and Access Management, minimizing downtime and expediting the recovery of critical data and services.

Ensure Entra ID data is always secure and available

Druva's 100% SaaS Solution provides a simple and efficient way to ensure you can recover your Microsoft Entra ID objects quickly, avoiding costly disruptions and reputational damages to your organization. By storing data in logically air-gapped storage fully hosted by Druva, ensure your Entra ID directory services can be restored efficiently in the event of cyber threats, data loss, misconfiguration, or accidental deletion.

Boost your platform and data security

Druva's Entra ID support in the Data Security Cloud provides an essential addition to our suite of supported workloads. Druva delivers autonomous data security with a 100% SaaS, fully managed platform to safeguard your data from any threat. Get comprehensive protection across diverse environments — data centers, SaaS apps, cloud-native workloads, and end-user data. Our unique approach ensures robust security and improves Incident Response and Remediation (IRR). With Druva, data security becomes autonomous, all from a unified platform.

Get full coverage for all your Microsoft data

Level up your Microsoft workload security. In addition to Entra ID, safeguard your data across Azure VMs and Microsoft 365 applications — SharePoint, OneDrive, Exchange Online, Teams, and Planner — with ease. With the agility of SaaS, deploy rapidly, scale dynamically, and manage seamlessly alongside other data sources on a unified platform. Experience peace of mind with secure air-gapped storage and robust data governance at your fingertips.

Why Druva?

100% SaaS, fully managed solution

Druva's Microsoft Entra ID protection is a 100% SaaS, fully managed solution, offering efficient, secure, and logically air-gapped storage for backups of Microsoft Entra ID Objects, alongside Microsoft 365, and Azure VM, and other cloud resources.

¹ [Microsoft Digital Defense Report 2023](#)

Complete data security for Entra ID objects

Druva provides a policy-based approach to protect and secure common Entra ID objects, such as Users, Groups, Roles, Devices, Enterprise Applications, Application Registrations, Administrative Units, and Conditional Access Policies.

Go beyond basic object recovery

Druva doesn't just recover Microsoft Entra ID objects; it restores their settings and relationships too. Customers can breathe easy knowing vital relationships like group memberships are restored along with the objects.

Object comparative restores

Druva provides capabilities to compare objects between snapshots, enabling users to swiftly recover specific data points or compare the current state with previous backups through comparative restores.

Key features

Protect containers with objects (including settings and relationships)

- **Users and relationships** — Druva provides a policy-based approach to automatically protect user objects and their associated metadata. Restores users along with their relationships, such as organizational hierarchy and reporting structures, ensuring continuity.
- **Groups and memberships** — Safeguards group objects and maintains the integrity of group memberships. Enables rapid recovery of groups with their exact member lists intact, crucial for maintaining access controls and operational workflows.
- **Roles and associations** — Protects role objects and their associations with users and groups. Ensures that role-based access controls are quickly restored, maintaining security and compliance post-recovery.
- **Devices (view / download only)** — Offers backup of device metadata and configurations. Provides capabilities to view and download device information to facilitate governance and compliance requirements.
- **Enterprise applications** — Protects enterprise applications by backing up application objects and their settings. Allows recovery of enterprise applications to their configured states, including permissions and connected services.
- **App registrations** — Secures application registration details, including client IDs. Restores app registrations with exact configurations, preserving essential integrations and access privileges across applications.
- **Export and Import backed-up data** — Ability to export the backed-up Entra ID as a JSON file and import it into a new Entra ID instance via PowerShell.
- **Administrative Units** — Protects administrative unit objects with their properties, memberships, and delegated roles, ensuring organizational structure and scoped administration are preserved.
- **Conditional Access Policies** — Safeguards conditional access objects with their properties, assignments, and access controls, enabling seamless restoration of security policies and enforcement rules.

With Druva, businesses can quickly restore Entra ID services, ensuring continuity and resilience against cyber threats and misconfigurations. Druva is among the first in the industry to meet this demand, filling a customer need, and addressing core IAM needs. Overall, the addition of Entra ID support strengthens Druva's comprehensive data security suite for Microsoft environments, enhancing user experience, operational efficiency, and market competitiveness.

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 industry's leading SaaS platform for data security, 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 Security 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](#).

Security Posture and Observability

Druva's posture and observability capabilities provide a real-time overview of your data security posture and deep observability into how your data has changed. Fortify the security of data in your backup environment and accelerate incident response with enhanced security insights into your data.

The Challenge

Ransomware has evolved into one of the most disruptive threats facing enterprises today. Attackers are no longer satisfied with encrypting production systems — they are deliberately targeting backup environments, understanding that recovery is the last line of defense. By corrupting backups, delaying detection, and hiding in the environment for weeks or even months, adversaries ensure maximum damage when they strike.

Unfortunately, most organizations are relying on traditional security tools that were designed to secure the perimeter, not enable fast recovery. These tools, often siloed from backup operations, can detect anomalies but rarely help IT teams identify which data is clean and recoverable. This disconnect means early warning signs are missed, and recovery is slowed when time is most critical.

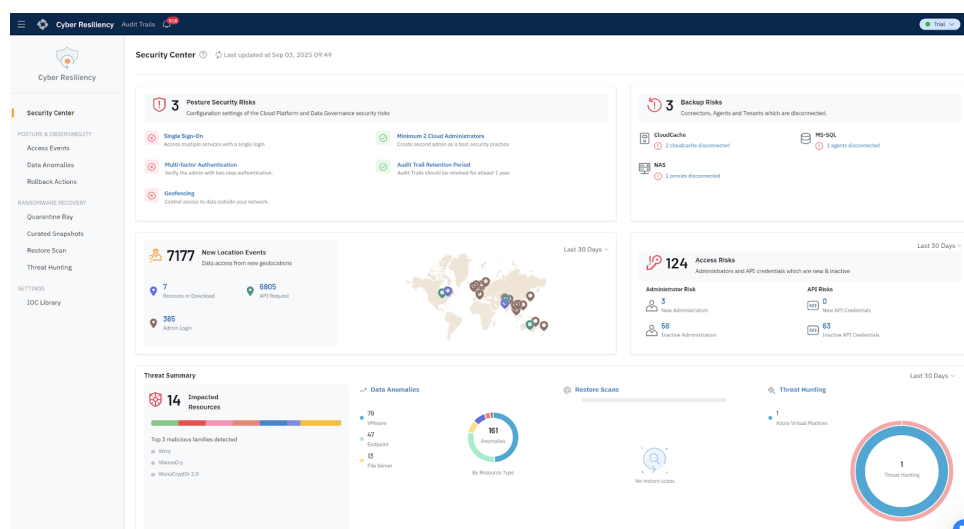
IT and security teams now operate under an assume-breach mindset. They are investing heavily in detection and response, but without a direct connection to the backup environment, their response capabilities remain limited. When the attack's primary target is data itself, the ability to simply restore backups is no longer sufficient. Clean data must be rapidly identified, validated, and restored — all while coordinating with security workflows.

The consequence of this gap is severe. Without deep integration between backup and security operations, recovery takes longer, downtime stretches into days or weeks, and the business faces escalating costs in lost productivity, revenue, and reputation. What should be an opportunity for resilience too often becomes an extended crisis.

Ensure Attack Readiness with Druva

Your backup data mirrors your primary data and is a rich source for improving your security posture and preparing for a potential attack. With Druva, continuously monitor your backup data and environment, respond to potential threats, and extend data to SIEM platforms for further insights with pre-packaged integrations.

Druva's Security Command Center dashboard ►



The Benefits of Integrated Posture and Observability

- Easily monitor the security posture of your backup environment and detect problems before they cause damage.
- Automate detection of access events and data anomalies within your backup environment such as restore requests from an unusual location, data encryption, unusual data deletion patterns, and more.
- Prevent accidental or malicious deletion of business-critical backup data despite compromised credentials.
- Enhance SecOps time-to-value with out-of-the-box, prepackaged SIEM integrations.

Key Features

- **Access Events Dashboard and Alerting** — Get relevant situational awareness about backup activity. A security event dashboard makes it easy to see unusual activity or drill into details about who has accessed your backup environment and data — administrators, users, and APIs, whether access occurred from a usual location, what occurred (e.g., backups or restores), and investigate alerts for data anomalies.
- **Rollback Actions** — With traditional disk and cloud storage systems, once an administrator deletes your backup data, it is gone. Only Druva allows you to roll back the deletion of backup data, using self-serve capabilities. Druva Rollback Actions can restore deleted backup data from a secure cache for up to 7 days — accessible only to you.
- **Data Anomaly Detection** — Druva uses AI/ML to detect malicious backup activity—such as deletions, modifications, or encryption—by analyzing data behavior to uncover ransomware. This capability spans endpoints (workstations, servers, NAS), virtual machines (VMware ESXi/vSphere), and cloud workloads (M365, SharePoint). Deployment is flexible: agentless for zero-touch, cloud-based protection without credentials or complex setup, or agent-based for deep integration with storage and file server infrastructure.
- **Recovery Intelligence** — Allows users to visually identify ideal restore points based on anomalous data activity, presence of IOCs, and observance of encryption activity.
- **Pre-Packaged Security Integrations and APIs** — Extend security event alerts and data into SIEM tools with one of several pre-packaged integrations or with Druva APIs. Some examples include:
 - Monitor compliance to geo-based data access and restore policies and API requests from new locations
 - Track user access patterns to recover data and unauthorized login attempts
 - Create alerts from pre-built rules to trigger pre-configured playbooks
- **Security Command Center** — Gain real-time visibility into your security posture with comprehensive risk assessments, including a Cyber Resilience Scorecard that validates proper configuration of critical resilience features. Unlock deep insights into risks across cloud platform security (e.g., administrators without MFA), data compliance, backup reliability (e.g., disconnected agents), and data access (e.g., users, APIs). Take swift, corrective action directly from a centralized command center.

You can not prepare for today's advanced threats and tomorrow's risks without including security posture and observability into your daily operations and security toolset. Trying to build and maintain this capability on your own becomes one more integration effort to maintain. The Druva Data Security Cloud delivers automation, unique data insights, and pre-built interactions to ensure your organization is attack-ready.



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 nearly 7,500 customers, including 75 of the Fortune 500, Druva safeguards business data in an increasingly interconnected world. Visit druva.com and follow us on [LinkedIn](#), [X \(formerly Twitter\)](#), and [Facebook](#).

Keep Sensitive Data Secure and Compliant

Druva's sensitive data governance solution offers a holistic approach, empowering organizations with enhanced visibility, consistent policy enforcement, and proactive risk mitigation to navigate data governance confidently.

The challenge

Organizations face mounting challenges in data governance. Stricter compliance requirements from courts and governments increase the compliance burden, alongside high costs and risks of penalties for non-compliance. Litigation is becoming more common and highlights the need for robust data governance. Fragmentation of data sources across physical and cloud environments compounds the issue, hindering centralized data management. Existing point solutions often lack comprehensive oversight.

Non-compliance of sensitive data can devastate your business in the following ways:

- **Financial** — Cost of litigation, investigation, and regulatory fines
- **Legal** — Legal action associated with customer data loss/theft
- **Trust and reputation** — Loss of customer trust and/or reputational damage
- **Operational** — Downtime and/or revenue loss as a result of data breach

What is sensitive data governance?

Sensitive data governance provides visibility of compliance breaches associated with end-user data in your organization. It enables your team to proactively track, monitor, and get notified of data compliance risks in your organization, across endpoints including laptops, desktops, and mobile devices, emails, and cloud platforms like Microsoft 365 and Google Workspace.

Druva empowers your team with deep data visibility and complete control

Druva enables sensitive data governance via a holistic approach, empowering organizations with enhanced visibility, consistent policy enforcement, and proactive risk mitigation to navigate data governance confidently.

The solution helps organizations monitor, track, and notify users of data compliance risks. It can report compliance violations for sensitive data in email bodies, subjects, and attachments. The feature can also help organizations:

- Comply with regulatory and compliance requirements
- Stay ahead of compliance violations
- Manage legal holds
- Reduce the time and cost associated with eDiscovery requests

Druva allows administrators to report compliance violations for sensitive data found within emails' bodies, subjects, and attachments. This capability is accessible through the Sensitive Data Governance Dashboard, which displays emails containing sensitive data and enables administrators to download these emails in EML file format for further review.

Once enabled, Sensitive Data Governance provides several key functions. Administrators can define what constitutes sensitive data and scan user data for compliance violations or potential risks. The feature allows for the location of end-user data that has breached compliance policies, facilitating the generation of non-compliance reports. These reports include visual representations to help indicate the company's adherence to compliance regulations, making it easier to maintain and monitor data governance standards.

Accelerated response to policy violations

- **Non-compliant file and email reports** — Druva enables the simplified and automated generation of reports to identify the users, data sources, and files that violate your organization's compliance policies. These reports will help you investigate potential risks of a data breach. They also help you to get in touch with the respective end users to get them to protect their sensitive data. For more information, [read more on generating a report](#).
- **Legal hold** — Based on the investigations conducted following the non-compliance report, you may choose to place relevant users on Legal Hold within Druva, if they have access to at-risk sensitive data. For more information, [learn more about creating a legal hold policy](#).

Key features

- **Centralized sensitive data governance dashboard** — Provides an easily navigable federated view by file name, date modified, user ID, sensitive data matched, and policy violated. This dashboard lets you quickly access and track compliance violations.
- **Non-compliance reporting** — Subscribe to compliance reports that automatically email to subscribers when potential data risks are discovered.
- **Predefined, customizable compliance templates** — Choose from predefined templates such as HIPAA, GLBA, and PCI, or customize your own. Druva will automatically scan, identify, and alert the organization of risks.
- **Intuitive dashboard, simplified administration, and powerful admin controls.**
 - Tamperproof audit trails with complete visibility of administrative changes to compliance policies.
 - Thresholds for sensitive data enabling the immediate response to critical violations.
 - Ability to scan files based on MIME types to cover against rogue or malicious end users.
- **Take actions to resolve compliance violations as per your incident response process.**
 - Ability to quarantine violations which will disable downloads and restores of files and email for Druva end users from the web.
- **Global and regional support with pre-defined templates.**
 - Support for sensitive data relevant to the US, UK, Germany, Australia, and South Africa, as well as sensitive data classified per global regulations.
- **Download files or emails for offline review.**
 - Download files and emails for offline review before taking remedial actions to avoid potential data breaches.

Druva's Sensitive Data Governance solution minimizes the risk of non-compliance and associated penalties while improving data quality. The solution ensures organizations have heightened visibility and control over gathered data, facilitating integration, interoperability, and effective management throughout the data lifecycle. Additionally, it provides valuable insights, empowering businesses to optimize their data strategies for maximum impact.

druva Sales: +1 888-248-4976 | 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 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](#).