Druva for Microsoft 365 Backup & Cyber Resilience

As your organization relies more heavily on Microsoft 365, protecting this business-critical data from loss, corruption, and cyber threats is non-negotiable. While Microsoft ensures infrastructure availability, it doesn't guarantee data security and recoverability. That's your responsibility. Druva provides a 100% SaaS-based, air-gapped, and scalable protection for Microsoft 365 that's purpose-built for today's cyber resilience demands.

The Challenge: Microsoft's Native Protection Isn't Enough

According to Microsoft's Digital Defense Report 2024, over 600 million cyberattacks target the Microsoft ecosystem every day. Yet native Microsoft 365 tools offer only basic retention, not true backup. The risk is real—21% of organizations report data loss despite having M365 backup policies, and 70% of ransomware incidents specifically target backups. Alarmingly, 43% of ransomware victims saw their backups encrypted, leaving them without a clean path to recovery. This widening gap between attack volume and protection capability exposes organizations to critical risks. As a result, customers often report the following experiences:

- **Short Retention Periods:** Microsoft 365 retains deleted data for only 14 to 93 days, with no flexibility to extend, leaving you unprotected once the window closes.
- **No Granular Recovery:** Native tools lack the ability to restore specific emails, files, or chats, forcing inefficient, broad rollbacks that disrupt users and delay recovery.
- **Ransomware Lockout & Malicious Deletions:** Without air-gapped or immutable backups, ransomware can encrypt or erase both live and backup data, making clean recovery nearly impossible.
- **Malicious Insider or Admin Threats:** A compromised or rogue admin can change retention settings or delete both primary and backup data, with no way to undo or trace the damage.
- **Operational Complexity:** Managing protection across Microsoft 365 workloads requires multiple admin consoles and scripts, making recovery slow, error-prone, and resource-intensive.

The Solution

Druva delivers a fully managed, 100% SaaS data protection and cyber resilience platform, purpose-built to secure Microsoft 365 against ransomware, insider threats, accidental deletion, and compliance risks. It provides resilient protection across a wide range of Microsoft workloads, including Exchange Online, OneDrive, SharePoint, Teams (including private chats), Planner, Groups, Entra ID, and more, all managed through a single, scalable platform.

Key Features & Benefits

Data Backup & Retention

- **Automated Backups**: Create custom backup policies to define backup and retention schedules, and automate Microsoft 365 backups with Druva, ensuring consistent, policy-driven protection across all workloads.
- **First Full, Forever Incremental Backups**: Create just one full backup. Druva's global deduplication ensures all future backups are incremental, saving time, bandwidth, and storage without compromising protection.
- **Air-gapped, immutable backups**: Druva stores Microsoft 365 backups in an isolated, air-gapped architecture with built-in immutability, preventing unauthorized access or tampering. The backups can be stored, retained, and managed within a specific country or region to meet enterprise latency and data residency requirements.
- **Smart Backups**: Druva's Smart Backup detects and protects only changed SharePoint content, reducing API calls and resource consumption.
- **Performance Optimization with Auxiliary Apps:** Dynamically deployed microservices scale out backup operations, optimizing backup performance intelligently to avoid throttling.
- **Lightning-fast Backup & Restore**: Druva's Microsoft 365 Backup Express solution delivers high-speed, large-scale recovery for Exchange, SharePoint, and OneDrive — with zero throttling and ultra-low RPOs/RTOs.

Data Recovery

- **Self-Serve Restore:** Users can independently restore Microsoft 365 data without relying on IT administrators.
- **Point-in-Time & Granular Recovery**: Quickly locate data using metadata search or select the specific snapshot to perform full or granular recovery of emails, folders, calendars, and files.
- **Flexible & Secure Restores**: Recover data to alternate locations, maintain a tamper-proof audit trail for legal compliance, and leverage APIs for programmatic restore automation.

Security & Privacy

- **Advanced Encryption**: Druva uses enterprise-grade digital envelope encryption (256-bit TLS in-transit and AES 256-bit at-rest) to secure Microsoft 365 backup data, ensuring maximum data privacy and security. It also supports Bring Your Own Key (BYOK) for added control using AWS KMS keys. Druva separates data, metadata, and encryption keys for added protection, ensuring that sensitive user data remains inaccessible to administrators.
- **Data Immutability**: The Data Lock feature prevents any modification or deletion of backups, ensuring true data immutability.
- **Strengthen Security Posture**: Enforce conditional access policies to align with Microsoft Entra ID restrictions, ensuring secure and compliant authentication. Monitor sensitive activities through built-in audit logs, analyze detailed reports for end-to-end visibility, and leverage real-time insights from the Security Center dashboard to proactively manage risks and strengthen your security posture.
- **Data Anomaly Detection**: Druva's patented AI-driven anomaly detection feature identifies suspicious activity, empowering organizations to respond swiftly and protect their critical data assets from cyber threats.
- **Quarantine Snapshot:** Automatically isolate suspicious files during Microsoft 365 backups to prevent unauthorized access or restoration. Enable secure, compliant recovery with admin-led investigation and control.
- **Recover Lost Data**: Druva's rollback feature enables swift recovery from ransomware or accidental data loss by restoring Microsoft 365 content to a known-good state from a secure cache retained for up to 7 days.
- **SIEM Integrations:** Druva captures every download and restore action, providing Microsoft Sentinel with detailed data insights to accelerate threat detection, investigation, and response - including deep integration with Copilot Security for AI-powered analysis.

Ransomware Recovery

- **Always-On Threat Monitoring:** Druva's Managed Data Detection and Response (MDDR) service helps you stay ahead of cyber threats with 24/7/365 real-time surveillance and AI-driven detection, accelerating response and ensuring clean recovery.
- **AI-Guided Investigation:** Druva's Dru Investigate feature uses AI-powered investigation and deep backup telemetry to help IT admins and security teams investigate cyber threats within their backup environment.
- **Unlimited Retention**: With unlimited retention for Microsoft 365, Druva enables recovery from clean snapshots, even if ransomware has been present for months.
- **Federated Search for Investigations**: Druva's federated search allows security teams to track infected files, analyze attack scope, and investigate events across Microsoft 365 users, devices, and storage.
- **Curated Recovery**: Druva creates tailored snapshots with the cleanest, safest file versions for seamless OneDrive and SharePoint restores.

eDiscovery & Legal Hold

- **Unified Legal Hold**: Druva enables proactive collection and preservation of Microsoft 365 and endpoint data with an electronic chain of custody. You can also preserve data belonging to departing employees, ensuring it remains available for current and future eDiscovery needs without incurring ongoing Microsoft 365 licensing costs.
- **eDiscovery Ecosystem Integration**: Druva integrates with leading cloud-native eDiscovery tools (Exterro, OpenText) to collect, preserve, and upload relevant data for legal review, analysis, and production.
- **Federated Search Capabilities**: IT admins can perform unified searches across Microsoft 365 and endpoints to locate sensitive data, support compliance, and streamline legal, forensic, and ransomware investigations.

Compliance

- **Comprehensive Compliance Support**: Druva offers built-in support for key global regulations like GDPR, CCPA, HIPAA, and FedRAMP, with proactive alerts and remediation for potential violations. Druva platform is also compliant with SOC 1, ISAE 3402, SOC 2, SOC 3, ISO 27001, PCI DSSLevel 1 (Cloud), and HIPAA regulations.
- **Customizable Governance Policies**: Use Druva's predefined compliance templates to create custom governance policies that meet both industry regulations and internal compliance requirements.
- **Data Governance & Defensible Deletion**: Address compliance violations by securely deleting prohibited data to support "Right to be Forgotten" requests under regulations like GDPR Article 17.
- **Retention & Security Certifications**: Ensure compliance with data-retention and disaster recovery regulations, while benefiting from certifications like SOC 2, ISO 27001, and PCI DSS Level 1.

Next Steps

Check out the Microsoft 365 solution page to discover how Druva closes your data protection gaps.

- Explore how Druva protects Microsoft Azure and the broader ecosystem: Visit the Webpage
- Try Druva's data security for Microsoft 365 for yourself: Tour the Product
- Get started with Druva with a 30-day free trial

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 for Microsoft Dynamics 365

Simplified, Resilient & Efficient Protection for Enterprise CRM Data

Protect the heartbeat of your business operations. Empower your organization with Druva's Dynamics 365 data protection solution—secure, compliant, and efficient.

The challenge

As organizations increasingly centralize their business-critical enterprise resource planning (ERP) and customer relationship management (CRM) applications data in the cloud, the need to efficiently safeguard this data becomes essential. Data loss due to accidental deletion, corruption, or cyberattacks can disrupt business continuity, lead to compliance issues, and result in financial losses. Microsoft's native backup and protection for its Dynamics 365 ERP and CRM application offers limited protection, leaving businesses vulnerable as a result of the following:

- **Inadequate Data Protection**: No air-gapped copy, and restoring an entire instance is costly and time-consuming
- **Compliance Risks**: Limited retention (28 days for production / 7 for sandbox) introduces compliance risks
- **Operational Inefficiencies**: Manual, error-prone recovery processes, leading to downtime and lost productivity
- **Data Risks**: No alerts for data corruption or deletion.

The solution

Druva for Microsoft Dynamics 365 simplifies tackling the critical challenges organizations face with cloud-based CRM data.

Tackling inadequate data protection, Druva offers granular recovery options for individual entities, relationships, records, and metadata, ensuring precise, cost-effective restorations without the need for time-consuming instance-level recovery.

Customizable retention policies extend data availability beyond Microsoft's limits, while anomaly checks through record comparison allow users to identify unexpected changes like bulk deletions, helping organizations avoid accidental or malicious data loss and stay compliant with regulatory requirements.

Druva also improves operational efficiency through automated workflows, which streamline backup and recovery processes, reduce manual errors, and boost productivity by freeing IT teams to focus on high-priority tasks.

To mitigate risks from data corruption, deletions, and cyber threats, Druva provides air-gapped backups, isolating data in the Druva Data Security Cloud to ensure data integrity and security. Addressing Microsoft's shared responsibility model, Druva gives organizations an independent, reliable backup system that protects critical data even during service outages. Together, these features provide a robust, resilient, and compliant data protection solution, securing Dynamics 365 data while enhancing operational continuity and reducing the burden on internal teams.

Key features

Druva's solution for Microsoft Dynamics 365 offers organizations the benefit of granular recovery options that enable precise and accelerated restoration of individual entities, records, relationships, and metadata, minimizing downtime. Customizable long-term retention policies align with business and compliance needs, while the search and compare feature allows quick identification of changes or anomalies. Flexible restoration to sandbox environments allows testing or restoration directly to production for seamless data verification and integrity.

Why Druva?

Security

Recovery-ready, always: Data is isolated from the customer's environment to protect against malware and ransomware. This approach guarantees business resilience with automated, fast recovery, while simplifying compliance through enhanced data visibility, control, and customizable retention policies to meet strict regulatory standards.

Simplicity

Guarantee clean recovery and prevent reinfection: Automatically populate sandboxes with quality data; set up workflows to minimize errors during data copy and maintain CRM relationships. Test data before recovery into production environments to ensure integrity and prevent reinfection.

Savings

Reduce total cost of ownership: Eliminate operational overheads and enable granular recovery to avoid the higher storage costs associated with full restores in the native solution.

One cloud-native solution, full data security for all your Microsoft apps

Protecting Microsoft data is multifaceted. Druva offers enterprise-grade backup and security for all your Microsoft apps, including Microsoft 365, Teams, Exchange Online, SharePoint, and OneDrive — as well as Dynamics 365, Azure VMs, and Entra ID. Our 100% SaaS platform ensures data security and accessibility, addressing critical gaps and enhancing data retention policies. With just one simple solution, Druva provides comprehensive and scalable data security you can rely on across your entire Microsoft environment — with an emphasis on interoperability and ease of use.

To learn more, visit:
druva.com/solutions/microsoft-dynamics-365

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

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 identities[1]. 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 Microsoft 365 Backup Express

Utilize Microsoft 365 Backup Storage with Druva Microsoft 365 Backup Express, seamlessly integrated within the Druva Data Security Cloud.

The challenge

Business continuity is a critical concern for many organizations. When evaluating backup and restore solutions, what truly matters isn't just the backup itself, but the flexibility you have to manage that data to meet operational and cyber recovery objectives, as well as data governance needs.

The solution

The Druva Data Security Cloud enhances Microsoft 365 data protection by addressing critical gaps in both native and other third-party platforms. Druva enables customers to unify end-user data across endpoints and the cloud for simplified search and legal holds, and ensures seamless data management with enhanced retention and accelerated recovery capabilities. Druva Microsoft 365 Backup Express offers customers an additional protection and storage option.

*Not currently supported via Microsoft 365 Backup Storage

Druva Microsoft 365 Backup Express is best suited for rapid recovery of large data volumes, making it perfect for large-scale Microsoft 365 environments. Seamlessly protect and restore 100+ TBs of data or 10,000+ objects across Exchange, SharePoint, and OneDrive. With your data securely stored in Microsoft Storage, Druva offers ultra-fast backup and recovery, as well as built-in Microsoft Entra ID support, all effortlessly managed through the Druva Data Security Cloud.

Why Druva?

Druva Microsoft 365 Backup Express offers organizations of all sizes an alternative solution for protecting critical Microsoft 365 data with ultra-fast backup and recovery capabilities and data storage in the Microsoft cloud.

Key features

Protect Critical Data:

Back up all or select SharePoint sites, OneDrive accounts, and Exchange mailboxes within the Microsoft 365 trust boundary.

Lightning-Fast Recovery:

Restore Exchange, SharePoint, and OneDrive data in bulk to a previous point in time with rapid speeds of 1 to 3 TB per hour.

Entra ID Protection:

Safeguard and recover your Microsoft Entra ID objects with Druva's backup solution, ensuring business continuity and resilience against disruptions.

Unified Management:

Centralized control for Microsoft 365, other SaaS apps, hybrid workloads, and cloud workloads like Azure VMs.

Customer Choice:

Select the right Microsoft 365 Backup solution based on your recovery time objectives (RTO), ensuring it aligns with your organization's specific needs and priorities.

Druva Microsoft 365 Backup Express highlights our dedication to advancing data security within the Microsoft ecosystem with our comprehensive Data Security Cloud.

End-to-end security and compliance for all your Microsoft 365 data

With Druva, you can also safeguard additional data across Microsoft 365, including Microsoft Teams, and close cyber resilience gaps. The Druva solution provides extensive features such as granular recovery, eDiscovery, legal hold, Managed Data Detection and Response (DDR), and Curated Recovery. Advanced security and incident response capabilities can identify unusual data activity, quarantine infected backups, and ensure that only the most recent and cleanest data is restored, allowing you to minimize downtime from security threats.

To learn more, visit druva.com/solutions/microsoft-365-backup-express

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

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.

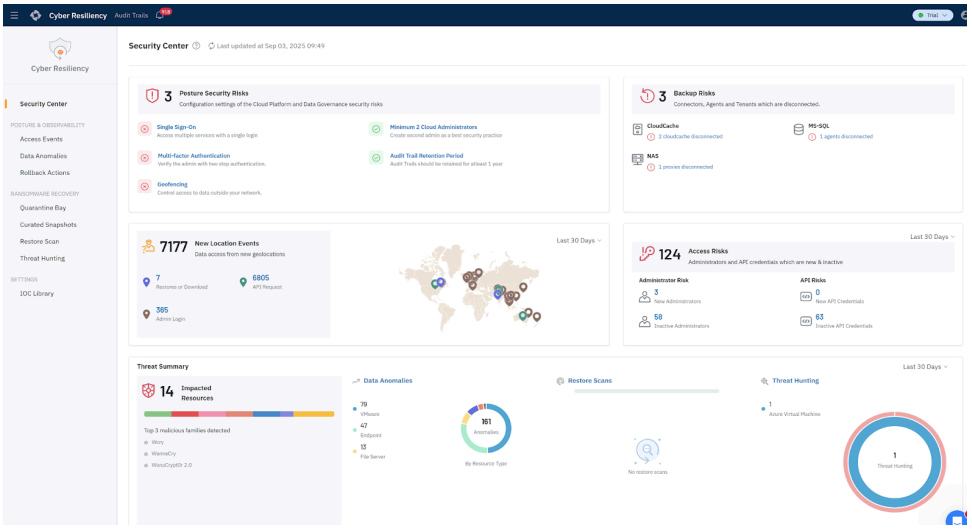
Unfortunately, most organizations are relying on traditional security tools that were designed to secure the perimeter, not enable fast recovery. These tools, often siloed from backup operations, can detect anomalies but rarely help IT teams identify which data is clean and recoverable. This disconnect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

CROWDSTRIKE | Microsoft Sentinel
paloalto NETWORKS | splunk>
Trellix | Microsoft Entra ID
sumo logic | BetterCloud
okta | servicenow
exterro | BOCADA

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