druva

A Modern Approach to Cyber Resilience

Secure by Design	MDDR with 24x7 Monitoring	Auto-tuning & Self-Healing	AI-powered & GenAI Supported	Out of Box Integrations	$10M DRG

Whitepaper
Q426-20600

Introduction

Cyberattacks targeting data continue to pose significant financial and operational risks, with the average cost per breach rising to $4.4 million globally in 2025 (IBM Security, "Cost of a Data Breach Report 2025). As businesses increasingly rely on data as a strategic asset, the consequences of data breaches—ranging from financial loss and operational downtime to reputational damage—have become more severe. The evolving threat landscape, exemplified by incidents like the SolarWinds attack and the Colonial Pipeline ransomware, has made safeguarding data a top priority across industries. Worldwide end-user spending on security and risk management is projected to total $240 billion in 2026, an increase of 12.5% from 2024, according to a new forecast from Gartner, Inc. Yet, even with the added investment in security, bad actors continue to find new ways to exploit vulnerabilities.

With diversified risks, data protection's role has evolved from a passive last line of defense to an active security partner in responding to and recovering from key threats. Four main risk types have emerged: availability, user, cyber, and process. Availability risks, such as those to hardware and applications, require continued attention to prevent data loss. User threats, like malicious exfiltration, have become more serious, especially with the rise of AI, which increases 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 handling across the entire data lifecycle.

The Evolution of Data Protection: From Recovery to Comprehensive Cyber Resilience

In today's dynamic environment, organizations must prioritize securely managing their data to ensure availability, prevent loss, maintain integrity, and protect privacy. Effective modern strategies must go beyond traditional perimeter-focused security measures to include deep data insights, observability, and tracking of data changes to drive comprehensive incident identification and response. Organizations need to ask themselves how each technology in the data lifecycle is contributing to threat detection, rapid response, and intelligent recovery to enable a more resilient and adaptive security posture. This is especially true for those using legacy data protection vendors, where security innovation has fallen short in solving for modern risks.

Historically, data protection has focused on mitigating the risks associated with infrastructure and application downtime. Organizations have invested heavily in disaster recovery measures to ensure business continuity during system failures or natural disasters. However, the rapid rise of cyber threats—including targeted attacks, malware, ransomware, and data exfiltration and data governance requirements — has necessitated a shift in data protection's role to expand beyond its traditional backup and recovery boundaries to encompass capabilities for:

Data Protection, Availability, and Fidelity: Ensuring that data remains accessible, accurate, and free from corruption or tampering. This means maintaining data integrity during transfer, storage, and processing.

Governance, Risk, and Compliance: Providing robust policy creation, controls, and monitoring mechanisms to meet regulatory requirements and maintain the trust of customers and stakeholders. Regular audits and compliance checks ensure adherence to standards.

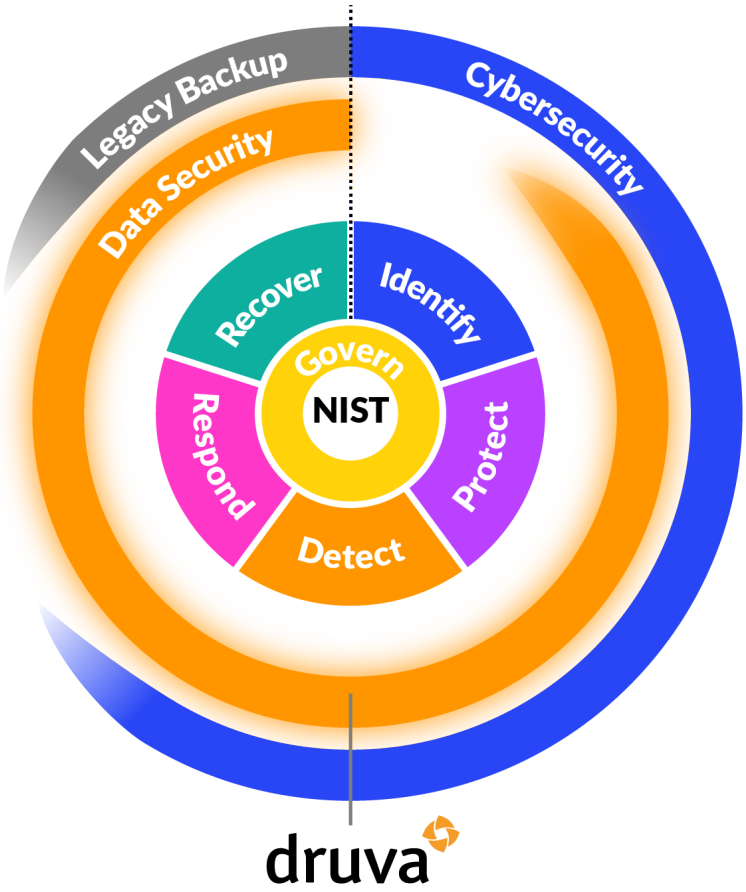
Data Insights and Observability: Discovery and visibility into data assets, their location, and usage patterns to identify potential risks and anomalies. For example, knowing where sensitive data resides and who accesses it can prevent unauthorized data access.

Enhanced Threat Detection: Utilizing advanced analytics and machine learning to promptly identify unusual data patterns that can indicate a sophisticated cyber or insider threat.

Accelerated Cyber Response, Investigations, and Recovery: Implementing tools and processes to quickly investigate and contain security incidents, minimizing the impact of a breach and ensuring rapid recovery of critical data. Rapid response protocols can mean the difference between a minor incident and a major data breach.

An ideal, modern cyber resilience solution incorporates these elements, enabling organizations to more effectively protect data, ensure business continuity, and navigate the complexities of today's IT landscape. This holistic approach to data security helps avert potential financial loss, legal penalties, and irreparable reputation damage. However, most data protection vendors have lagged behind on innovating for security, lacking the comprehensive capabilities that could significantly drive results. As a result, organizations are often forced to cobble together multiple-point solutions to address the full spectrum of security needs, leading to increased complexity and potential security gaps.

A Comprehensive Approach: Druva Data Security Cloud



The Druva Data Security Cloud leads the industry as a pioneering SaaS-first and fully managed platform, engineered to secure and recover data from a wide array of threats with its innovative cloud-native architecture. Druva employs a zero-trust security model and ensures the highest level of security across all workloads. The platform provides a comprehensive solution encompassing data protection, cyber response and recovery, and eDiscovery and compliance.

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

Druva's Data Security Cloud features air-gapped storage and control planes for managing data protection across environments, including on-premises servers, virtual infrastructure, cloud workloads, SaaS applications, and endpoints. As a cloud-native solution, organizations avoid the overhead of managing on-premises hardware, achieve scalability on-demand, and get the cost advantages provided by global deduplication built on object storage.

Foundational Security Across All Workloads

The Druva platform unifies workload visibility, policy management, and security capabilities to provide organizations with a comprehensive solution for safeguarding their data, while also enhancing control and governance to ensure compliance with industry regulations.

Key benefits include:

- **Data Encryption:** Druva encrypts data at rest with AES 256-bit encryption and in transit using industry-standard TLS encryption. Source-side deduplication and object storage further scramble stored data, making it impossible for unauthorized parties to access or decipher sensitive information.
- **Data Lock and Immutability:** Data can be locked by policy, preventing it from being modified, deleted, or overwritten for a specified period, guaranteeing that data remains intact and recoverable, even if an attacker gains admin access to the system or if an insider attempts to tamper with the data.
- **Role-based Access Control (RBAC):** Administrators can define and enforce granular access controls based on user roles and responsibilities, ensuring that users can only access the data and functions necessary for their specific job requirements.
- **Consistent Policy Enforcement:** Apply data protection policies uniformly across all environments, minimizing gaps or inconsistencies and ensuring that data protection standards are met.
- **Full Audit Trails:** Druva maintains a detailed audit trail of all activities, providing visibility into data protection events. This extensive auditing helps organizations demonstrate compliance with relevant regulations and standards, while also supporting forensic investigations in the event of a security incident.

Druva's advanced data protection capabilities enable organizations to safeguard their critical assets while ensuring compliance with industry standards, providing a secure and reliable foundation for cyber resilience.

Cyber Response and Recovery

As cyber threats become increasingly sophisticated and frequent, robust cyber resilience is essential for any organization. Druva's Data Security Cloud offers a comprehensive solution for cyber response and recovery, combining 24/7 Managed Data Detection and Response (DDR) with Safe Mode, advanced Security Posture and Observability (SP&O), Accelerated Ransomware Recovery (ARR), Recovery Intelligence, Data Anomaly Detection (Agentless), Cyber Resilience Scorecard, Threat Insights, and ReconX Labs. Druva's latest security enhancements empower customers with intelligence-driven cyber resilience. Detect anomalies quicker, accelerate recovery, and be confident your team can handle any threat.

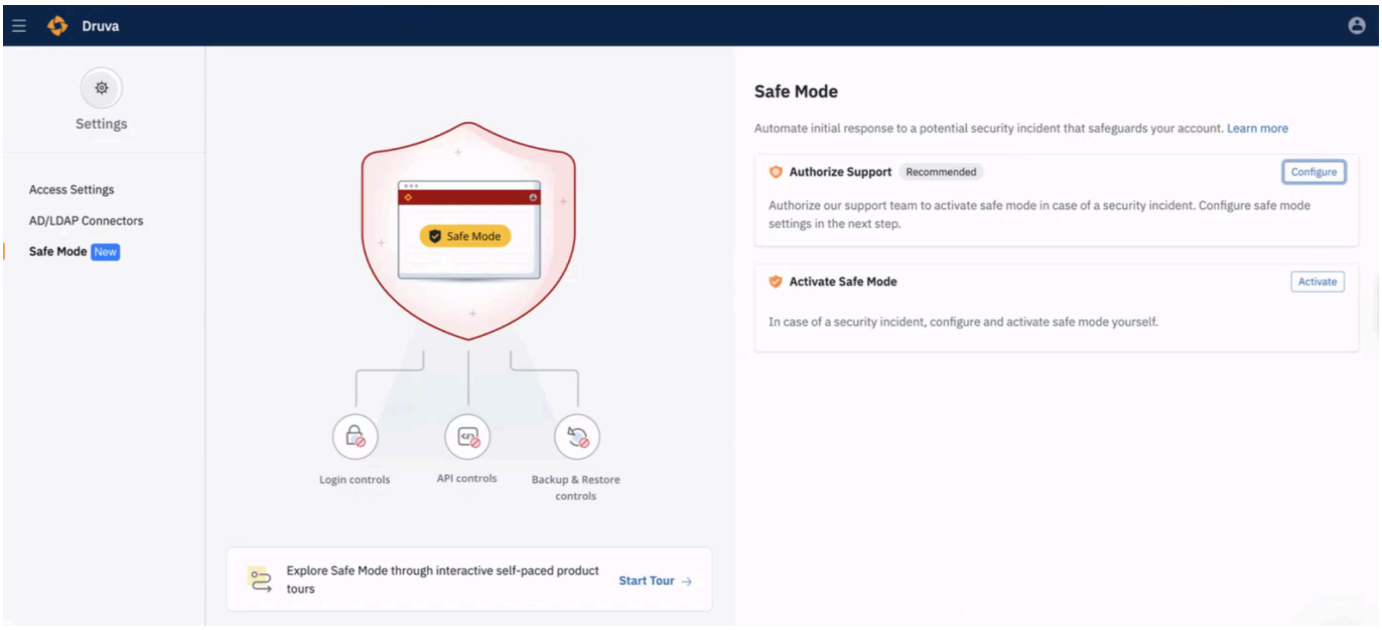
Managed Data Detection and Response (DDR) with Safe Mode

Druva Managed Data Detection & Response (MDDR) is a natively delivered service that combines advanced monitoring and threat detection capabilities, utilizing backup telemetry, with expert-driven analysis and response—enabling organizations to respond to threats promptly. Druva's analysts act as an extension of the customer's Incident Response team, examining alerts and conducting detailed analyses to eliminate false positives. Upon threat verification, Druva's team takes immediate action by notifying the customer and implementing proactive measures to secure and, if necessary, roll back compromised data. They provide actionable insights and pre-built or customized runbooks to help customers thoroughly understand and mitigate security incidents during response and investigation.

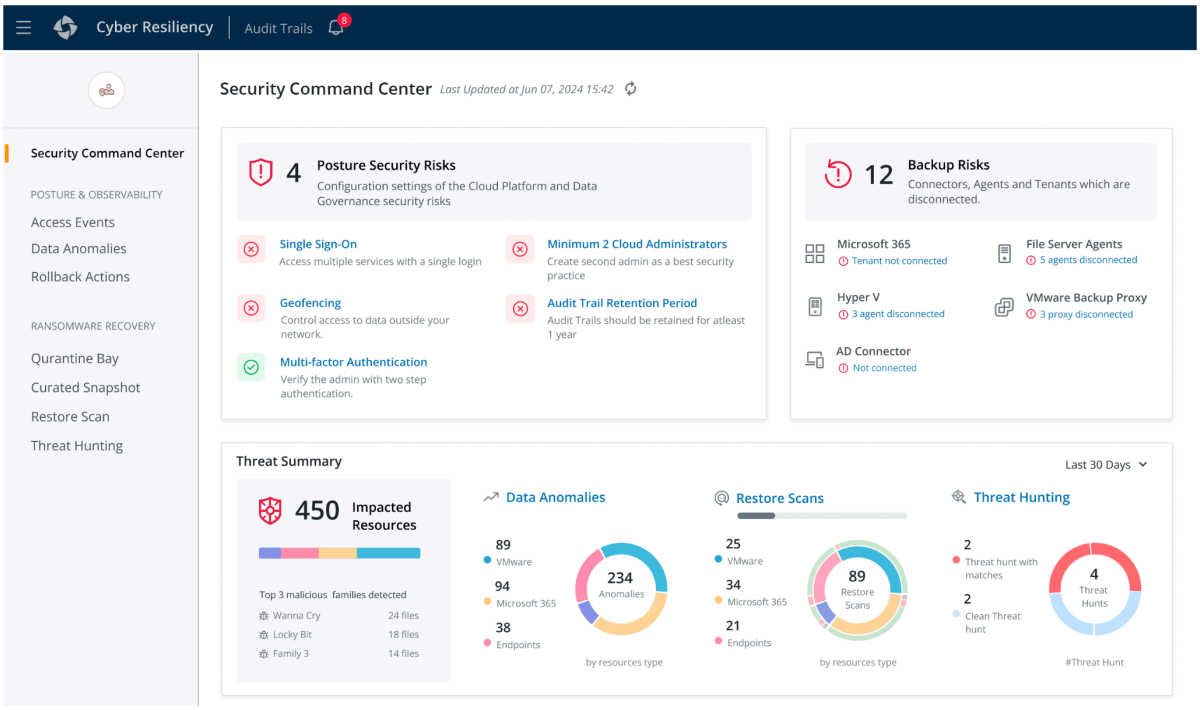
Adding a crucial layer of protection, Druva's MDDR with Safe Mode acts as an instant "emergency brake" for your environment. Safe Mode allows administrators to immediately lock down the environment—blocking deletions, pausing restores, and restricting compromised access before any damage can spread. This capability, combined with 24×7 monitoring and expert verification, accelerates containment and enables clean recovery. Druva MDDR with Safe Mode is the industry's first automated threat response and containment solution delivered from a true SaaS model, designed for fast and reliable cyber recovery. The result is faster response times, fewer reinfections, and recovery you can trust.

Druva's Managed DDR goes beyond traditional data protection, providing a unique advanced security service.
Key benefits include:

- **24x7x365 Continuous Attack Monitoring:** AI-powered and human-enhanced real-time monitoring and threat detection across your entire backup environment, enabling early detection of ransomware and other malicious activities.
- **Actionable Intelligence:** Leveraging advanced analytics, machine learning, Druva's vast metadata repository, and expert analysis, quickly identify threats and quarantine them to prevent spread or reinfection. Eliminate threats from backups and primary environments with defensible deletion.
- **Accelerated Incident Resolution:** Collaboration with your incident response team to investigate, respond, and reduce incident resolution time using backup data logs, telemetry, and pre-built playbooks.
- **Minimized Downtime:** Custom recovery strategies designed in collaboration with your IT and security teams, with assistance through the entire recovery process to minimize downtime.
- **Safe Mode:** Automatically lock down the environment by restricting access and enforcing controls (e.g., pausing backups/restores, blocking deletions) while investigation proceeds. [Take a product tour!]



Security Posture and Observability (SP&O)



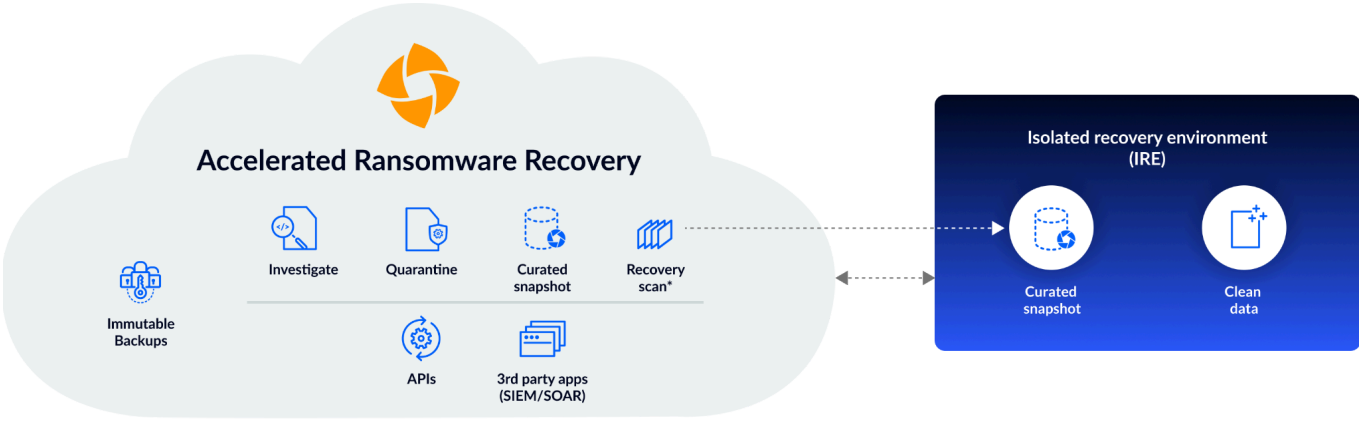
Druva's SP&O service provides a prioritized view of data risks across backup snapshots, enhancing the detection and response to threats, including data exfiltration, backup data deletion, insider threats, and ransomware activity.

With continuous monitoring capabilities, advanced analytics, and machine learning-driven anomaly detection, SP&O helps organizations proactively detect and respond to potential threats to their critical data before they cause significant damage.

Key capabilities include:

- **Security Command Center Dashboard:** Get real-time total platform security posture risk assessments and insights into; cloud access posture risks, Connector(s)/ Agent(s) and Tenant(s) risks, prioritized Threat Summary, and backup data access risks. Take corrective actions directly from the dashboard.
- **Real-time Event Visibility:** Gain near-real-time situational awareness of suspicious activities and data anomalies across your environment. Leverage AI/ML-driven detection for unusual patterns in backup activity, data access (including API and console access), and potential threats across Endpoints, Virtual Machines (VMs), SaaS apps (M365, GWS), File Servers, and NAS workloads.
- **Rollback Actions:** Restore deleted backup data, profiles, endpoints or user accounts from a secure cache for up to 14 days (default setting is 7 days), accessible only to authorized users. Policy edits to circumvent the retention period are guarded against with 4-eye authentication confirmed via Druva support engineers.
- **Pre-Packaged Security Integrations and APIs:** Extend security event alerts and data into SIEM tools or use Druva APIs to monitor compliance, track user access patterns, and create custom alerts.
- **Compliance Reporting and Auditing:** SP&O provides pre-built compliance reports and dashboards that offer visibility into backup data risks, user activities, and data access patterns, helping organizations meet regulatory requirements and maintain a strong security and governance posture.

Accelerated Ransomware Recovery (ARR)



*Scan for malware with Druva or 3rd party file IOCS.

Druva's ARR capabilities are designed to help organizations overcome the risks associated with ransomware attacks by offering a comprehensive suite of tools for investigating, quarantining, and recovering. Leveraging ARR, organizations can significantly reduce downtime, minimize data loss, and accelerate recovery times in the event of a ransomware attack. At the core of this solution are guided recovery workflows that provide step-by-step guidance and automated processes, helping organizations navigate the complex recovery process while minimizing the risk of human error and ensuring critical data is restored quickly and accurately.

Key capabilities include:

- **Automated Backup Data Scanning:** Continuously scan backup data for signs of malware infection or anomalous activity to identify potential ransomware infections early and take swift action to contain the threat.
- **Quarantine:** Quickly quarantine backups at the snapshot, device, and VM level within the Druva console, or automate the process using third-party integrations and Druva APIs.
- **Restore Scans:** Filter out malware using AV scans with Druva-supplied and custom file indicators of compromise.
- **Curated Recovery:** Algorithms rapidly identify and recover the most recent clean versions of files across an incident timeline. This approach minimizes data loss at scale, accelerates the recovery process, and eliminates the need for tedious, traditional granular recovery methods.
- **Sandbox Recovery and Testing:** Leverage Druva's cloud-based platform to safely test and verify recovered data in an isolated environment before full restoration, ensuring clean, malware-free recovery and minimizing the risk of reinfection during the recovery process.
- **SIEM/SOAR Integrations and APIs:** Accelerate time to value with pre-packaged integrations for security information and event management (SIEM), and security, orchestration, automation, and response (SOAR), or build custom automated playbooks using Druva APIs.

Learn more about how Druva improves incident response workflows, enabling organizations to significantly enhance their security posture, remediation, and recovery capabilities. Druva offers pre-packaged integrations and the ability to build custom automated playbooks using Druva APIs. These integrations accelerate time to value, enabling organizations to respond more effectively to threats and ensure rapid recovery from incidents.

Recovery Intelligence

Druva Recovery Intelligence strengthens your backup and recovery by embedding security insights directly into the restore process. It helps organizations confidently recover data by detecting threats early and ensuring restore points are safe, reducing risk and downtime.

Key capabilities include:

- **Real-time threat detection: I**dentifies anomalies, encryption, malware, and Indicators of Compromise (IOCs) in backups.
- **Safe restore point selection:** Highlights clean recovery points to avoid reinfection.
- **Faster recovery:** Speeds up decision-making with automated security context and reduces manual analysis.
- **Built-in security:** Integrates with existing workflows without extra infrastructure or agents.
- **Comprehensive visibility:** Provides restore point and file-level insights for better risk assessment.
- **Supports compliance:** Generates logs and reports for audits and incident response.

By combining backup, threat intelligence, and policy enforcement in one SaaS platform, Druva Recovery Intelligence ensures secure, efficient, and resilient cyber recovery for modern enterprises.

Data Anomaly Detection (Agentless)

Ransomware attacks have evolved into sophisticated operations that target an organization's data directly, often bypassing traditional security defenses. While tools like EDR and SIEM monitor endpoints and networks, they lack visibility into what happens to the data itself. Data anomaly detection fills this gap by continuously analyzing backup data to identify unusual activity such as unexpected deletions, modifications, or encryption—signs of a potential attack in its earliest stages. Druva's cloud-native solution offers seamless integration with existing security frameworks, providing faster detection and response without adding complexity.

Druva's Data Anomaly Detection offers:

- **Zero-touch, simplified deployment** across endpoints, on-premises, and cloud.
- **Enhanced security** by eliminating guest OS credential dependencies.
- **Scalable cloud-based indexing** that doesn't impact system resources.
- **Rapid alerts** within one hour of backup completion for quick action.
- **Cost-effective** infrastructure utilization for predictable expenses.

Cyber Resilience Scorecard

Druva's Cyber Resilience Scorecard simplifies the complex task of protecting organizations against ransomware by providing clear, guided insights into their security posture. It addresses key challenges such as fragmented tools, rising complexity, and knowledge gaps by offering an intuitive dashboard, intelligent readiness scoring, and step-by-step configuration guidance. This approach empowers administrators to easily identify vulnerabilities, prioritize essential security controls, and maintain compliance through automated audit trails, making cyber resilience achievable and effective.

Benefits of Druva's Cyber Resilience Scorecard:

- **Provides immediate visibility** into security posture through an intuitive, interactive dashboard.
- **Categorizes security controls** into mandatory and additional groups for clear prioritization.
- **Uses a color-coded scoring** system for quick assessment of configuration status.
- **Offers guided configuration** with contextual help and one-click setting modifications.
- **Eliminates confusion and accelerates time-to-value** for both new and existing users.
- **Automates audit trail tracking** to simplify compliance and security audits.
- **Helps close security gaps** faster and strengthens defenses against ransomware.
- **Reduces management complexity** by consolidating security configuration in a single interface.

Threat Insights

Druva Threat Insights transforms immutable backups into a continuous security layer — defending backup data proactively with Threat Watch and enabling rapid investigation and cleanup with Threat Hunting. By scanning directly in the backup stream (without added infrastructure or data movement), uncover long-dwell threats, prevent reinfection during recovery, and validate clean restore points with confidence.

- **Threat Watch (Proactive):** Automated, continuous scanning of backup snapshots with retrospective rescans when new IoCs emerge — plus quarantine and reporting for recovery readiness.
- **Threat Hunting (Reactive):** On-demand searches across backup metadata to identify scope and timeline, quarantine infected restore points, and defensibly delete compromised files so recovery can proceed from clean data.

ReconX Labs

Druva's ReconX Labs is a dedicated security research unit focused on advancing ransomware preparedness and recovery. By leveraging real-world data and expertise, it delivers actionable threat intelligence integrated into Druva's platform to enhance detection, accelerate clean recovery, and improve cyber resilience. The initiative includes the community-driven Ransomware Recovery Hub and new capabilities such as agentless anomaly detection and AI-powered threat monitoring, helping organizations reduce complexity and respond faster to ransomware incidents.

Key capabilities include:

- **Real-world ransomware intelligence** for improved defense and recovery.
- **Integrated threat detection** and automated clean recovery.
- **Community resources** with recovery playbooks and best practices.
- **Agentless, zero-touch anomaly detection.**
- **24x7 AI-driven threat monitoring** with instant containment.
- **Cyber Resilience Scorecard** for continuous readiness assessment.
- **Visual recovery insights** for reliable restore point selection.
- **Reduced complexity, cost, and response time** in ransomware defense.

Identity Resilience

With 90% of cyber breaches leveraging compromised credentials, the identity layer has become a direct pathway for systemic disruption. Druva Identity Resilience is purpose-built to defend identity as the foundational layer of the modern enterprise. By centralizing protection across Okta, Entra ID, and Active Directory, we unify fragmented IdP environments from a single, immutable SaaS platform. This approach empowers organizations to surgically restore environments to verified, clean states while precisely identifying and purging persistent threats to enhance overall cyber-readiness postures. By rapidly re-establishing access for both human and non-human identities (NHIs), Druva ensures operational certainty when it matters most–reinstating a trusted, functioning identity layer while unblocking recoverability for all downstream applications, workloads, and systems.

Underpinning this resilience is Druva's "identity-aware" foundation, powered by the MetaGraph, delivering the deep visibility and continuous modeling other tools miss. By continuously analyzing access, relationships, and behaviors over time, we provide a clear lens into identity-driven attacks, replacing guesswork with high-fidelity signals and telemetry. The result is more informed, evidence-based intelligence that empowers organizations to identify, contain, and recover from threats with absolute clarity and precision.

Governance, Risk, and Compliance

In today's stringent regulatory environment, non-compliance can lead to severe financial penalties and damage to reputation. Druva's Data Security Cloud empowers organizations to reduce compliance, regulatory, and legal challenges by enabling GRC teams to easily access data and streamline processes. The platform provides comprehensive capabilities for eDiscovery, legal hold, and sensitive data governance, ensuring that organizations can effectively navigate the complex landscape of data management and regulatory compliance with confidence.

eDiscovery and Legal Hold

Druva's eDiscovery and Legal Hold solutions work in tandem to minimize downstream review and processing costs, ensure data authenticity, and streamline the legal hold process across the organization. By reducing reliance on custodians and enabling proactive data collection, Druva helps organizations mitigate the risk of data destruction or spoliation and align with EDRM requirements.

Key capabilities include:

- **Preserve-in-Place Legal Holds:** Securely place legal holds on stored data, enabling IT to respond to legal inquiries quickly and identify custodians faster with federated search.
- **Proactive eDiscovery Data Collection:** Store data by date range and file type, preserve data across endpoints and cloud applications, and identify legal hold data across users, devices, and locations.
- **Chain of Custody Reporting:** Ensure data is fingerprinted for authenticity and meets legal hold defensibility, with metadata collected per DOJ and EDRM guidelines.
- **Streamlined Legal Hold Management:** Reduce reliance on custodians while minimizing the risk of data spoliation, streamlining the legal hold process across the organization.
- **Data Preservation Across Endpoints and Cloud Applications:** Preserve data across various data sources, ensuring a comprehensive approach to legal hold management.

Sensitive Data Governance (SDG) Strengthens Data Security Posture

Druva's SDG solution is the first of many innovations to come, addressing data security and compliance challenges, functioning as an effective DSPM tool. It provides a centralized dashboard for sensitive data governance with an easily navigable federated view, enabling quick access and tracking of compliance violations. The solution empowers organizations to discover, classify, and protect sensitive data while ensuring regulatory compliance.

Key capabilities include:

- **Data Discovery and Classification:** Automatically scan, identify, and classify sensitive data across various sources, providing visibility into data assets to understand risks and prioritize remediation efforts.
- **Centralized Sensitive Data Governance Dashboard:** Access an easily navigable federated view by file name, date modified, user ID, sensitive data matched, and policy violated, enabling quick tracking of compliance violations and overall data security posture.
- **Proactive Risk Management:** Subscribe to non-compliance reports that automatically email subscribers when potential data risks are discovered, enabling security teams to address data security and compliance issues quickly.
- **Automated Remediation Actions:** Implement actions to resolve compliance violations, such as quarantining files and emails to disable downloads and restores, helping to mitigate potential data breaches and prevent their recurrence.
- **Continuous Monitoring and Improvement:** Provide ongoing data insights and automation that enable security teams to maintain a strong data security posture, address issues promptly, and continuously improve compliance efforts.

By implementing Druva's advanced GRC solutions, organizations can enhance their compliance posture, reduce regulatory risks, and ensure the integrity and security of their data. In an era of stringent regulatory requirements and increased scrutiny, Druva's proactive approach to governance, risk, and compliance is essential for maintaining trust and meeting legal obligations.

Customer Story

achieve

"Achieve is a leader in digital personal finance, offering home equity loans, personal loans, and debt resolution, as well as financial education. Achieve is the consumer brand of Freedom Financial Network, LLC."

Challenge

- Needed a cloud solution to support remote workforce
- Christmas Eve ransomware attack left the team on high alert, needing to fully restore data at a moment's notice

Solution

- Druva delivered cyber resilience for 3,000+ employees, including all remote employees
- 100% SaaS allows for efficient restores and recovery no matter where employees are located

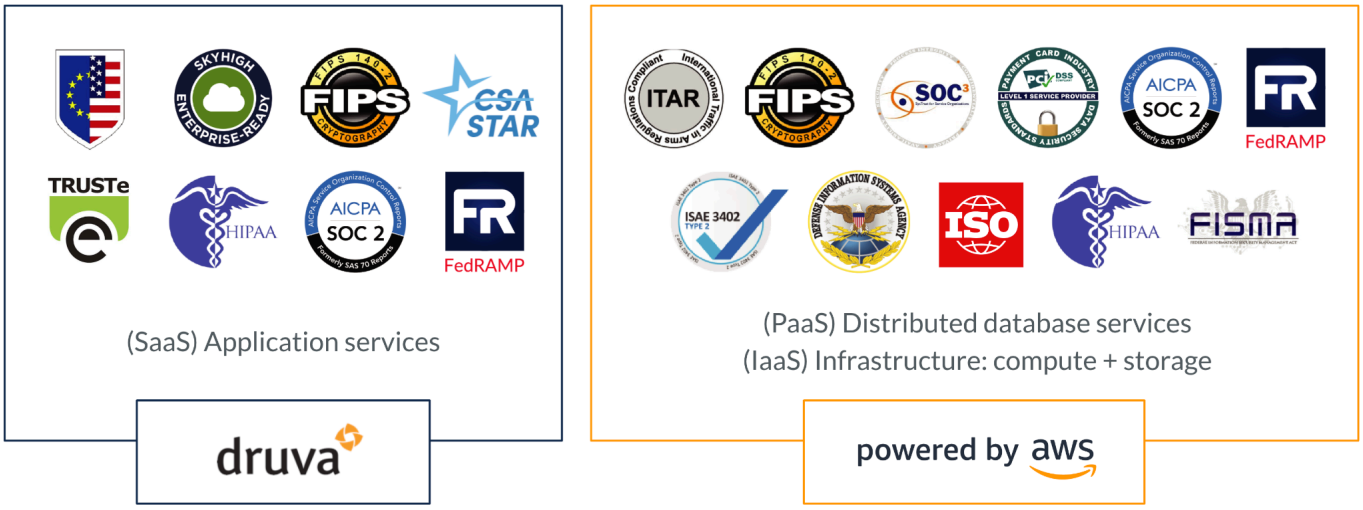
Results

- Just one hour to restore devices compromised during the attack
- 50% decrease in service desk requests and time spent resolving issues
- Seamless restore and recovery process — a key benefit for their hybrid workforce

druva

Druva's Data Security Cloud delivers a comprehensive, unified, and innovative approach to cyber resilience, empowering organizations to protect, secure, and govern their critical data assets effectively. By offering a secure SaaS architecture, advanced data protection capabilities, robust cyber resilience features, and streamlined governance, risk, and compliance functionalities, Druva enables businesses to navigate the complex landscape of modern data security with confidence.

Going Above and Beyond: Druva Attestations and Certifications



Druva's commitment to security extends beyond products and services, as the company continuously aligns itself with the latest industry standards. Druva's services are validated by a range of industry attestations and certifications.

These include:

- **CSA STAR:** Druva has achieved Level 2 certification in the Cloud Security Alliance's Security, Trust, and Assurance Registry (STAR) program, demonstrating a comprehensive approach to cloud security.
- **SOC 2 Type 2:** Druva has achieved and maintained Service Organization Control (SOC) 2 Type 2 audits for more than five years, validating the company's internal management and controls related to security, availability, processing integrity, confidentiality, and privacy.
- **FedRAMP:** As the first cloud backup provider to achieve Federal Risk and Authorization Management Program (FedRAMP) Moderate certification, Druva demonstrates compliance with the stringent US government security requirements for cloud service providers.
- **HIPAA:** Druva's platform is compliant with the Health Insurance Portability and Accountability Act (HIPAA), ensuring the secure handling of protected health information.

These certifications not only validate Druva's unwavering commitment to security but also establish the company as a trusted leader in the data protection and security industry.

To learn more about how Druva's certifications can benefit your organization and ensure the highest standards of data security, visit Druva's Trust Center or contact our team of experts today.

The Druva Data Security Cloud Advantage: Delivering Results

In today's digital landscape, where data is both invaluable and increasingly vulnerable, Druva's Data Security Cloud stands out by providing a single, secure, and scalable platform to tackle the complex challenges of cyber resilience. Built on a secure-by-design philosophy and cloud-native architecture, and featuring Managed DDR alongside advanced security capabilities, Druva instills confidence in organizations by safeguarding their data against sophisticated cyber threats. Its latest security enhancements further empower customers with intelligence-driven cyber resilience, enabling quicker anomaly detection, accelerating recovery, and ensuring teams are fully equipped to handle any threat with confidence.

Druva's comprehensive approach to cyber resilience, encompassing backup and recovery, proactive monitoring, threat detection, and rapid response to ransomware attacks, empowers organizations to focus on their core objectives with confidence. As cyber threats evolve, Druva's Data Security Cloud remains well-equipped to help organizations navigate the challenges of data protection with ease.

Next Steps

Take the next step in securing your organization's data with Druva's cyber resilience solutions. We help you protect your data, prepare for cyber attacks, and automate recovery processes to minimize downtime and risk. Discover how to strengthen your defenses and enhance your cyber resilience today.

Find data security blind spots with the **Cyber Resilience Maturity Model**. Answer 5 quick questions and receive your personalized cyber resilience score. Find security gaps and get strategies you can put into place NOW to be ready for cyber threats:

Assess Your Cyber Maturity↗

Tour the Druva product to see firsthand how we strengthen your data defenses and enable stress-free recovery:

Take a Product Tour↗

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