druva

White paper

Critical Steps for Data Protection and Scalable Recovery From Ransomware

How to recover faster and prevent data loss

Q424-20471

Backups are supposed to save you, so why is ransomware still a problem?

Ransomware is here to stay — in fact, it's become a thriving business with organized gangs and sophisticated approaches. In its 2023 Threat Report, cybersecurity firm Sophos notes that the cybercriminal economy has transformed into an industry unto itself, adopting an as-a-service model for an increasing scope of operations.

The antidote is preparation and a readiness to recover. But in this crucial area, most organizations fall short, despite rising awareness of the ransomware threat, by simply relying on traditional data protection measures, and increasing security expenditures.

Data recovery does not equal cyber recovery

IT teams play a critical role in an organization's ransomware response and recovery by managing the backup systems that enable data recovery. Meanwhile, the cybersecurity industry is focused on protecting their organization by identifying and detecting threats to primary data in real time. Security teams focus primarily on preventing access to all data and systems, and IT teams manage the systems and processes for business continuity and the backup data for cyber recovery. IT teams think of data protection as "backup," but have not traditionally leveraged data in incident response and some aspects of cyber recovery.

Having a strong security posture is a requirement for all organizations, but it does not translate to cyber resilience. While organizations have used backups to recover from cyber attacks, what's less frequently shared in headlines is the percentage of data loss and time to restore. It's much higher than you would expect. How much of your data you can recover and how quickly your business gets back up and running will depend on two things:

1. Having a certified clean recoverable data set and a functioning backup platform from which to recover
2. Your IT team's ability to collaborate with security efficiently and effectively under pressure and time constraints

Several research reports show that you can't pay to get your data back — for example, in its 2023 State of Ransomware report, Sophos reveals that:

> In 30% of attacks where data was encrypted, data was also stolen. Shockingly, this comes after 46% of organizations reported paying the ransom to help recover their data, and the average recovery cost climbing to $1.82M excluding any ransoms paid.[1]

Numbers like these underscore the risks in paying ransoms and the need to approach cyber recovery differently. Ransomware recovery readiness must be an executive priority that includes both security, IR, and IT teams. Recovery from ransomware and protection of your backup system should be embedded in your risk management process or entered in a risk log. The ability to demonstrate this capability and recover quickly with minimal data loss, can satisfy many IT, compliance, and board-level mandates. With proven security controls you can reduce the duration and cost of business disruption when security events or breaches occur.

Many organizations have security incident response plans, but very few have added ransomware recovery support to those plans, and even fewer have tested such plans. This guide aims to prepare you with the key principles you need to ensure a rapid and full recovery after a ransomware attack.

In this guide, you will learn about:

- What to consider when protecting your backup environment
- How cyber recovery is different than data recovery
- What IT should know about working with security on cyber recovery
- 5 ransomware recovery readiness gaps and how to close them
- Druva's approach to ransomware readiness and recovery

[1] "Sophos State of Ransomware 2023", May 2023

What to know about protecting your backup environment

Backing up your data is the first step to being able to recover – whether from ransomware or accidental deletion. When it comes to your backup environment, your choices have broad implications. Consider where you will store your backup data and how much you plan to manage yourself.

On-premises vs. Cloud vs. SaaS

Traditional on-premises backup solutions such as backup appliances or tape libraries have long been the default for many organizations. However, these on-premises solutions have well-documented security vulnerabilities that are being directly targeted by ransomware cybercriminals. In addition, the cost and complexity of deploying and managing these systems have driven many organizations to consider more modern approaches.

Cloud-based data protection solutions are where a customer runs on-premises backup software in a VM in the cloud. Cloud-based solutions are customer-managed products that still require the same number of security updates to the OS and backup application. They often require on-premises backup appliances. Server-based data protection solutions run in the cloud and face the same critical security challenges as on-premises solutions.

A SaaS-first solution eliminates hardware, software, and maintenance using a cloud-native approach. It is offered as-a-Service, with the SaaS vendor maintaining all backup infrastructure. An example is the Druva Data Resiliency Cloud, which is designed to eliminate the operational and management overhead of backup and recovery while optimizing data security and reducing cost. Features such as air-gapped, immutable backups come standard with a true SaaS delivery model.

Why ransomware recovery is different

While most organizations today encrypt their backup data, transmit it over secure networks, and replicate it to a different location, these measures neither fully protect their backup data from ransomware nor enable rapid recovery in the event of an attack. Ransomware recovery is different from traditional business continuity or disaster recovery events for several important reasons:

- IT and security teams need to actively plan and collaborate on ransomware recovery
- The backup system is also a target and is often compromised by ransomware
- When you can recover data is dependent on coordination with security and/or incident response teams (e.g., quickly sharing and accessing log data from different systems)
- Where you recover data may be different given the extent or nature of the breach
- Traditional recovery methods are not always effective because the data must be scanned or verified as clean by the security team.

Why the anatomy of a ransomware attack matters

Building data resilience and recovery capabilities requires you to understand the general anatomy of an attack. Attackers seek to get access to your data through a weak link. Usually, this starts with phishing attacks used to trick an employee into clicking a malicious link in an email or downloading malware. The goal is to establish a foothold in your environment. Next, an attacker will move laterally in stealth to understand your environment and identify critical data and systems. How they achieve their objectives is always evolving (e.g. encryption, wiper wear/deletion, or exfiltration), but the goal is to take the highest value data and systems hostage. Your backup environment is a top target for this reason because it is your last line of defense. If attackers are able to compromise your backup environment, the chances you will pay the ransom significantly increase.

What IT should know about working with Security on recovery

Assuming your IT organization has good data protection hygiene practices, ideally, you'll have immutable backup copies and files to recover after a ransomware attack. However, work needs to be done before you're ready to recover, including finding the source and extent of the infection. For a successful recovery, IT leaders should understand how security approaches recovery and the stages involved. At every step of the way, an IT team that is prepared can accelerate the response and recovery processes to get systems back up and running rapidly. Here are five recovery stages you should plan for:

1. Early detection and faster incident response with automation and integrations

Starting a conversation with the security team as part of the ransomware recovery preparation is important. There are areas where backup tools can fill coverage gaps and augment incident response. Backup security logs can be integrated into SIEM tools to augment the detection of user and data anomalies. Incident response and recovery playbooks and tools (e.g., SOAR tools) can be integrated with backup to accelerate response and remediation (e.g., quarantine backups during an incident or data recovery scans).

2. Different data sources require different workflows

Different data sources like files, VMs, and end-user data, which can include both endpoints (laptops) and SaaS data (M365) will require different workflows and recovery capabilities adding complexity to cyber recovery. For example, scanning VM backups requires file-level access to the virtual drive being scanned, but VMs are typically not backed up at the file level. This usually means you must restore all virtual drives for a given VM and mount them before they can be scanned. Endpoint data found on laptops has unique needs that are often overlooked in the effort to protect the crown jewels in the data center. While preventing reinfection and making data available for 100 laptops may be possible without automation, response and recovery outcomes will be much faster with orchestration and automation, especially as the number of endpoints grows into hundreds, thousands, or more.

3. Digital forensics

Before recovery can begin, the security team must contain the attack, perform digital forensics to assess the scope and extent of damage and ultimately remove all traces of malware. They will determine just where the attacker was in the network, and where malicious activity or data exfiltration occurred. They will then narrow the investigation to individual machines, and the attacker's tactics, techniques, and procedures (TTPs) should start to come into focus. Access to backup and security logs can accelerate this process. The incident response team might also quarantine backups to prevent accidental re-infection.

4. Finding the right restore point and clean backup data

Ideally, backup systems were isolated and the attacker was not able to encrypt the backup data. Even if backup data was not compromised by ransomware, the backups, which are copies of primary data, can contain both malware and encrypted data. Security will determine how long the attacker was in the network. Based on this decision, IT will need to determine the optimal recovery point to minimize data loss. Backup tools can also provide insights and automation to identify when encrypted files appear in backup data. Because an attack may contain different pieces of malware, inserted over time by an attacker, IT teams also need the ability to scan data at restore time.

5. Cleaning data and testing restored systems in a sandbox

The extent of compromise and the nature of the attack will dictate how and where you recover data. Security will frequently ask IT to use a sandbox or isolated recovery environment for recovery to ensure restored systems have no malicious ransomware on them before moving data to the production environment. Restoring systems in a sandbox environment typically requires rebuilding the critical infrastructure components required to run and manage applications such as VMware, Microsoft, or Nutanix clusters, database servers, and application servers. Often the public cloud can provide a fast and scalable environment for sandbox restores and fast migration to a production environment.

Because many or all of your systems and networks may be shut down due to an attack (or deemed "unsafe or uncertain" by the security team), you need to plan for these requirements. The next section will cover how to start building recovery readiness by closing common gaps.

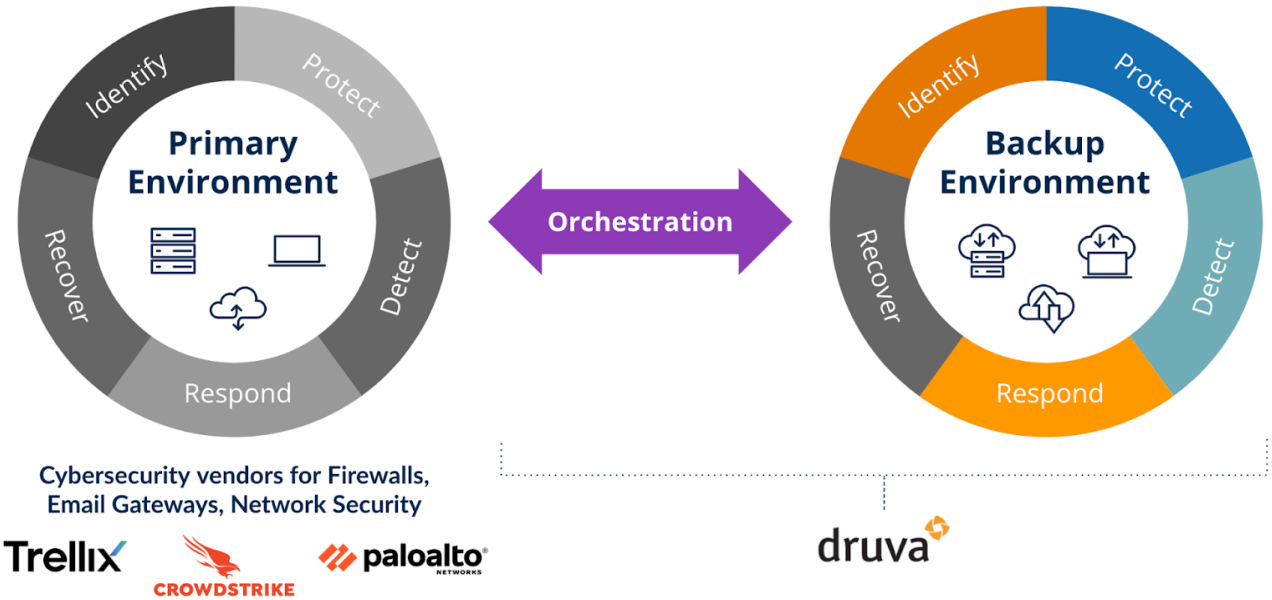
Ransomware is not just a security problem

IT operations teams and security teams need to collaborate on ransomware readiness and recovery. Because this is not a one-time exercise, an executive sponsor can be beneficial to ensure continuous collaboration, testing, and updates to the ransomware playbook.

5 ransomware recovery readiness gaps and how to close them

Many security teams leverage an established cybersecurity framework developed by the U.S. National Institute of Standards and Technology (NIST) in collaboration with other international agencies. The NIST framework identifies five cybersecurity functions: identify, protect, detect, respond, and recover.

Taking these five functions as a starting point, IT leaders can map out key points of collaboration to overcome recovery readiness gaps. The figure and table below show areas of responsibility for security and IT and indicate actions IT can take that will accelerate recovery.



Function	Security | Primary Environment	IT | Backups
Identify	• Develop an organizational understanding of cybersecurity risk to systems, data, & capabilities. • E.g. Identify the systems that are the most critical to protect.	• Align critical applications and protection policies with backup and security teams. • E.g. Make the backup platform a tier 1 application.
Protect	• Develop & implement the appropriate safeguards to ensure delivery of services. • E.g. Protect primary data with multiple tools and methods.	• Protect both your backup data and environment. • E.g. use air-gapped backups and immutability for data sets, establish pen-testing, automatic updates, and vulnerability monitoring for your environment.
Detect	• Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. • E.g. Security teams use many tools from endpoint detection and response (EDR) to SIEMs.	• Look for unusual activity in backup data (e.g., irregular data flows) and the environment (e.g., encrypted files, admin activity within the backup environment, deletions, etc.). • Maintain and monitor logs. Enable the security team to access backup data to support an incident investigation.

Respond	• Develop and implement the appropriate activities to take action regarding a cybersecurity event. 1. **Stop the attack** and monitor your success. 2. **Investigate and define** the blast radius of the attack. 3. **Begin remediation,** which includes a recovery phase.	• Ensure backup and security logs are available to incident response teams even if systems and networks are down. • Support file and indicator of compromise (IOC) scanning of backups at the point of recovery.
Recover	• Develop and implement appropriate activities to maintain plans for resilience and to restore impaired capabilities and services. • Ensure backup data is clean and validated before moving to production, relying on the IT team to execute. • E.g., Provide a day of infection, systems infected, key IOCs, etc. to IT.	• Malware re-infection is a frequent occurrence. IT needs to support backup quarantine, recovery scans, and integration with security tools to enable automation and rapid recovery. • Consider how you can avoid data loss if encryption occurs over time. Some vendors can curate a "golden snapshot" across multiple snapshots to reduce data loss.

This is an abbreviated summary of the NIST framework.

Backups are your last line of defense

Security teams think about ransomware protection in terms of detection, prevention, and investments like EDR/XDR, SIEM tools, and so on. Backup is not a first-class citizen in this world. It may be up to the IT team to help security teams understand the urgency of protecting not only primary data and systems, but also secondary systems such as backups.

NIST reminds us: **"Regular backups that are maintained and tested are essential to timely and relatively painless recovery from ransomware events.** Backups should be secured to ensure they cannot become corrupted by the ransomware or deleted by the attacker. The backups should be stored offline."

About Druva's approach to recovery readiness

Druva has pioneered a SaaS-first approach that has helped numerous customers recover from ransomware attacks. Our platform offers a cohesive framework to help IT teams ensure that they are ready to respond and recover with confidence and speed.

A 3 Pillar Approach to Ransomware Recovery Readiness

Autonomous Protection

Integrity & Availability of Platform & Data

- Druva hosted, fully-managed
- Automated updates and patches
- Inherently secure with access control, air gap, immutability, and encryption
- Adaptive experience

Rapid Response

Security Posture & Observability

- 24/7 continuous monitoring
- Sensitive data governance
- Unusual data alerts and audit logs
- Augmented incident response
- SIEM integrations

Guaranteed Recovery

Accelerated Ransomware Recovery

- Always-on recovery
- Clean data, on-demand
- Curated Ransomware Recovery
- Automated workflows
- Expert assistance

SOAR & SIEM Integrations with Security Solutions

How Druva accelerates ransomware recovery

The Druva Data Resiliency Cloud offers foundational security capabilities to customers guaranteeing their backup data and platform are fully protected and available. Additional features help customers better prepare for potential threats, regardless of their security expertise, with continuous security posture monitoring and anomaly detection. And patent-pending features like curated recovery automate recovering clean backups with minimal data loss.

Autonomous Protection

With data securely hosted and fully managed by Druva, businesses are free from the complexities of hardware and software management. The SaaS model ensures continuous optimization, self-healing, and automatic, regular updates, guaranteeing the platform remains at the forefront of data protection. Security is paramount, with access controls, end-to-end encryption, and ensuring customer backup data and control plane is isolated from threat vectors.

Rapid Response

Druva delivers actionable insights that accelerate business response to any incidents. With 24/7 continuous monitoring of the backup environment, coupled with proactive notifications and granular data logs, Druva enhances incident response capabilities. Druva offers built-in zero-trust security and integrates seamlessly with SIEMs, issuing alerts for data deletions, encryptions, and access activity. Empower your team to assess and minimize an incident's impact, all without disrupting production.

Guaranteed Recovery

In the event of a breach, automate recovery of clean and complete data, get back to business, and avoid reinfection. Curated recovery automatically reconstructs your latest clean data files into a single "golden snapshot," expediting the process of bringing your business back online with confidence. And non-disruptive malware scans and sandbox recovery help customers avoid reinfection. Dedicated support is readily available and free to assist with any and all recovery efforts.

Why Ransomware Recovery with Druva is Different

The Druva Data Resiliency Cloud is a SaaS-based data protection platform that transforms how teams manage and secure their data by removing the risk and operational overhead associated with managing multiple data protection platforms.

Secure by design:

Druva is a 100% SaaS-based platform that is not connected to your corporate network. With the full benefits of the cloud, you never need to buy or maintain any backup infrastructure and can scale up or down automatically without having to source and deploy new hardware. Patching, upgrades, and the rollout of new features take place automatically without any impact on the customer. As backup data is stored and managed by Druva, customers take advantage of a logical air gap to ensure their backups are always kept secure and inaccessible to ransomware and other threats. Druva leverages strong authentication and security protocols like single-sign-on (SSO), role-based access controls (RBAC), and multi-factor authentication (MFA) that meet government standards. It encrypts data in flight and at rest, uses unique, customer-specified AES-256 encryption keys (i.e., envelope encryption), and offers immutability with Druva Data Lock.

Industry-leading operational security:

Druva hosts a zero-trust platform and fully manages its availability and security with pen testing, automatic vulnerability scans, patching, and automatic upgrades. We take security and availability seriously and offer the Druva Data Resilience Guarantee with defined SLAs across five key risks — environmental, human, application, operational, and of course cyber risk.

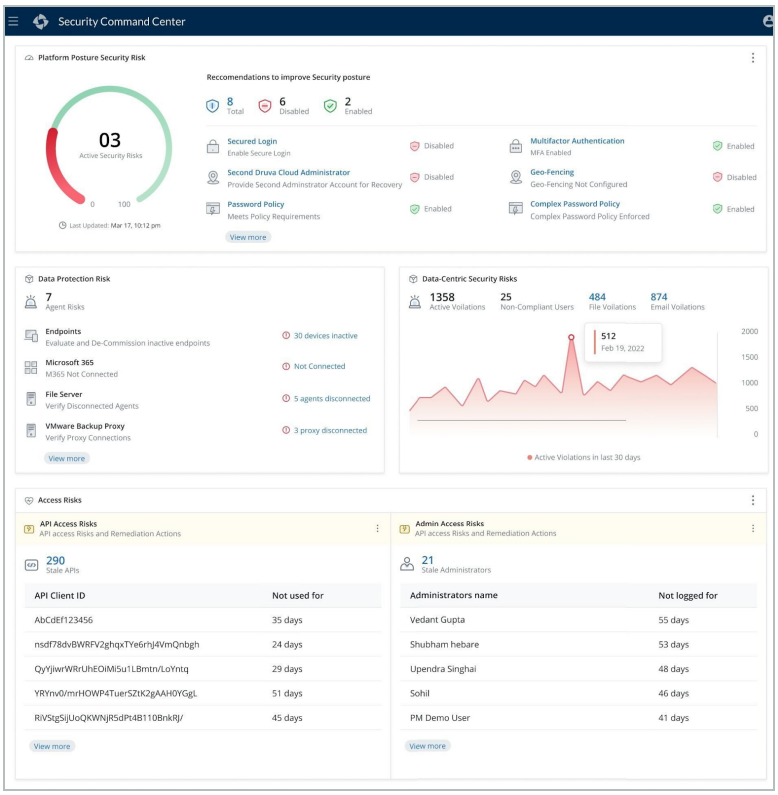
Continuous monitoring:

The Druva Cloud Ops team analyzes telemetry from each vertical and company size, uniquely identifying local and global trends daily. This team automatically monitors your account for bulk deletion events and contacts customers if an alert arises providing customers with the critical time window needed to rollback and recover deleted backup data.

Posture and observability:

Druva provides a centralized governance dashboard and security command center so that you can view your security posture and data risks at a glance and investigate details with a single click. Integrate Druva with your SIEM and SOAR tools. Key risk areas that can be monitored include:

- **Platform Risks:** SSO and MFA enablement, Geofencing, # of cloud admins, and audit trail retention
- **Data Access Risks:** APIs and users/admin activity or lack of activity (stale logins)
- **Data Protection Risks:** Disconnected agents or systems
- **Data Compliance Risks:** Insights into data compliance risks using Druva Sensitive Data Governance capabilities.



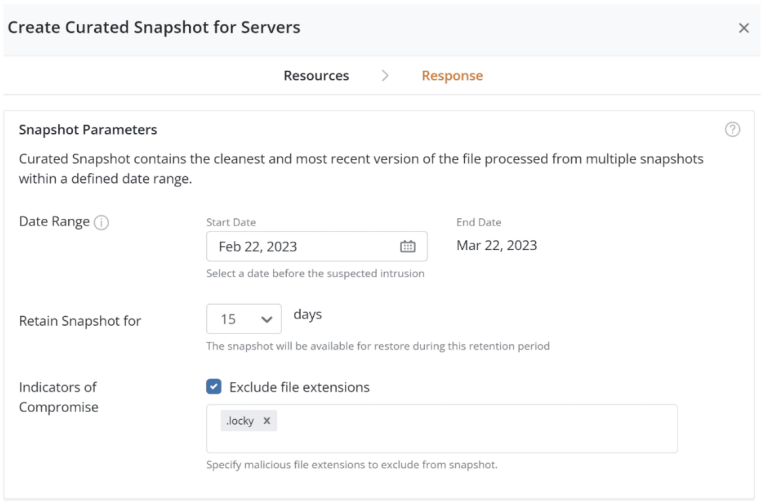
View your security posture with the Security Command Center Dashboard

Rollback deleted data:

Easily safeguard backup data from accidental or malicious deletion by configuring rollback windows and deletion reporting. Druva can maintain up to 7 days' worth of deleted backups in a secure cache.

Accelerated recovery:

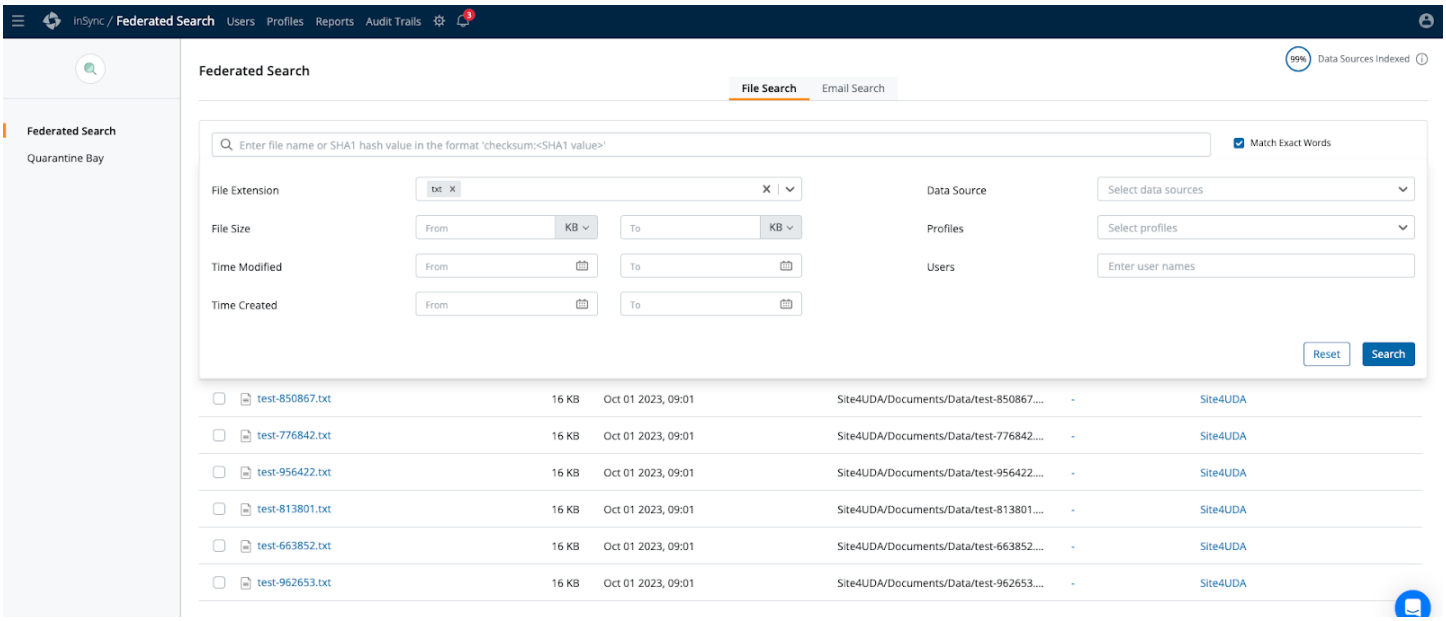
Druva provides unique capabilities to accelerate cyber recovery, including pre-built integrations with third-party tools to enable orchestration, the ability to quarantine infected systems and snapshots, scanning for malware and IOCs, and a patent-pending feature, curated recovery, to create the latest, cleanest, and safest scanned version to restore.



Curated recovery reduces data loss and automatically assembles the best snapshot over time

Forensics:

Leverage federated search capabilities to assist post-incident investigations. Druva ensures backup logs are preserved and accessible to aid forensics efforts.



Start your journey to ransomware recovery readiness today

Traditional backup and recovery environments are no match for today's ransomware attacks. IT needs to harden its backup infrastructure and seek ways to leverage that environment to support the security and resiliency goals of the company.

- Gain executive sponsorship, create and test plans for ransomware recovery readiness
- Align the backup environment with the organization's security posture
- Practice forensics and recovery in a sandbox or isolated recovery environment

The Druva Data Resiliency Cloud can kickstart your journey to ransomware recovery readiness. Druva customers who have been attacked by ransomware have directly experienced the value of Druva's ability to respond and recover from ransomware. Read the stories of Pyrotek, DMS Health Technologies, and six other Druva customers who made a full, speedy recovery from ransomware, and explore the full benefits of 100% SaaS on druva.com.

druva Sales: +1 888-248-4976 | sales@druva.com

Americas: +1 888-248-4976
Europe: +44 (0) 20-3750-9440
India: +91 (0) 20 6726-3300
Japan: japan-sales@druva.com
Singapore: asean-sales@druva.com
Australia: anz-sales@druva.com

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