druva

White paper

Five Steps to Ransomware Protection and Recovery

A comprehensive guide to implementing an effective data resilience strategy

Q422-20320

Introduction

The rise of ransomware has become a crisis that has crippled organizations world-wide. New strains of ransomware and other malware threats specifically target backup data for encryption or deletion, effectively destroying organizations' last line of defense. With more employees transitioning to working remotely, exposure to ransomware and the risk of infection are increasing at an alarming rate.

Ransomware is a form of malware that encrypts victims' data so threat actors can demand a "ransom" in exchange for a decryption key needed to unlock your data.

Even if the ransom is paid, there is no guarantee that the attacker will provide you with the decryption key. Some companies refuse to pay, relying on backup data to recover. However, according to Coveware, 26% of companies that have a backup solution in place at the time of the attack are still unable to recover their data.

Downtime, data loss, business disruption, and damage to brand credibility can be devastating. The U.S. National Cyber Security Alliance found that 60% of small businesses hit by ransomware go out of business within a year.

In today's diverse and distributed IT environment, restoring your organization's applications and data quickly in the event of a ransomware attack is a significant challenge. According to a Gartner analysis of clients' ransomware preparedness, over 90% of ransomware attacks are preventable with sound security fundamentals, including an effective backup and recovery strategy.

Reliable backup and recovery is a crucial line of defense against ransomware. Secure backup copies can empower companies to restore their critical business data and applications without paying a ransom. Backups are vital for data and applications that are particularly vulnerable to ransomware such as end-user data, NAS, file shares, virtual machines, and SaaS applications including Microsoft 365.

There are several data protection solutions in the market to help address backup and recovery, with well-orchestrated, built-in recovery mechanisms that automate manual processes to recover backup data quickly and easily.

Your business needs a data resiliency solution that does all of the following:

- Ensures data integrity and availability by protecting backup data from ransomware
- Enables you to operationalize security without overtaxing your IT team
- Empowers you get back to normal faster with orchestrated and automated recovery options

> **From the June 2021 White House memo on ransomware:**
>
> Backup your data, system images, and configurations, regularly test them, and keep the backups offline. **Ensure that backups** are regularly tested and that they **are not connected to the business network, as many ransomware variants try to find and encrypt or delete accessible backups.** Maintaining current backups offline is critical because if your network data is encrypted with ransomware, your organization can restore systems.

5 steps to protect your organization and limit the impact of ransomware

Druva's secure and robust cloud architecture can help you protect your business assets, limit the impact of ransomware, and accelerate recovery. To help you start, **here are 5 steps to help you improve your business resilience.**

1. Ensure data integrity and availability for key business assets
2. Operationalize security across primary and backup environments
3. Orchestrate response to automatically contain threats
4. Identify anomalous data and activities
5. Automate the recovery of complete and clean data

1) Ensure data integrity and availability for key business assets

In order to recover from ransomware (without paying the ransom), you must have a secure copy of your applications and business data. In this section, we will explore how to identify key workloads and protect them.

Identifying key workloads

The first step for any data protection strategy is to understand the full scope of the applications and data that needs to be protected. This includes the critical servers and applications that power your business in addition to the entry points where ransomware can attack (primarily your endpoints).

When assessing your data protection needs, consider these key areas for protection:

- **End user data** — the most likely source of a ransomware attack comes through social engineering of your end users. Endpoints (laptop, mobiles devices, etc.) and SaaS applications that hold your end user data (Office 365, GSuite, etc.) need to be protected in order to detect and limit the spread of ransomware.
- **Data center applications and data** — these systems are the true target of ransomware, and loss of access to these systems can critically impact your business. Protect the virtual machines, NAS systems, and databases that are critical to the health of your business.
- **Cloud workloads** — As the use of cloud computing on platforms like Amazon Web Services increases, it is mission critical to ensure that these environments can be restored quickly in the event that ransomware infects these systems.

Automating the data protection processes and policies for backing up your key assets ensures that you have up to date backups to facilitate a timely recovery. Configurable backup policies and pre-configured compliance templates assist you with defining the assets to protect, with associated compliance and retention policies as appropriate to your environment.

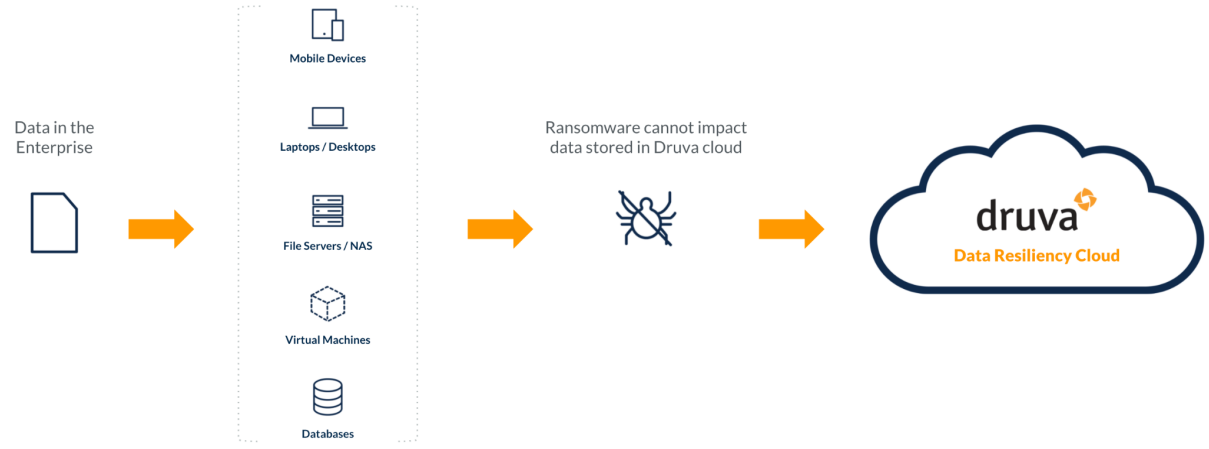
Data integrity

Identifying key assets to protect and automating your backup process is important, but you must also ensure that your backup data cannot be encrypted or deleted by ransomware. We'll discuss several ways to ensure security, including:

- Choosing a solution with malware resistant architecture
- The importance of access control
- How to implement zero-trust security

Malware resistant architecture

You need to choose a data resiliency solution that prevents ransomware from executing in the backup environment. To ensure your backup data is secure, look for a solution that provides air-gapped, immutable and encrypted backups.



Air-gapped backups and object based storage

Ransomware cannot execute in the Druva environment thanks to how the Druva Data Resiliency Cloud is built.

- There is no network or NTFS access to the Druva cloud. As a result, Druva backups are not accessible using OS/system credentials.
- Data is never stored as-is. Druva stores data as smaller application-aware blocks before being stored in an object store.
- Without access to an operating system, the malware cannot execute on its own. It cannot establish any communication with its command and control center for any further triggers or execution code.
- Druva's cloud environment is not based on Windows and does not depend on the direct-attached storage, Active Directory applications, or Remote Desktop Protocols typically used by ransomware.

As an extra layer of security, Druva retains deleted snapshots in an inaccessible cache for seven days so it is possible to restore data even if it has been deleted from the backup environment.

Encryption

Another key to security is encryption for data, both in flight and at rest. Druva Cloud Platform provides a secure, multi-tenant environment for customer data.

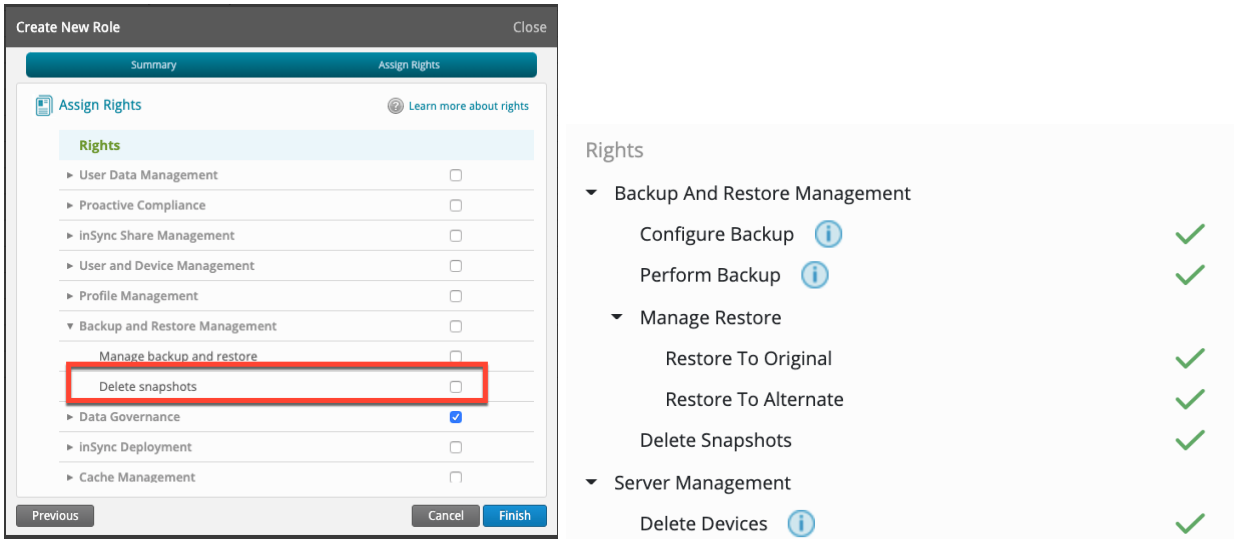
- Druva issues unique per tenant AES-256 encryption keys and offers encryption for data in flight and at rest. The use of one unique encryption key per customer along with customer held encryption keys, creates crypto-segmentation between customers, preventing data leakage.
- Druva stores the data by splitting it into blocks and deduplicating, with unique data blocks stored in Amazon S3. Metadata is stored in Amazon DynamoDB. Amazon EC2 provides the computational layer to enable elastic scalability.
- The application layer is separate from the data layer. As a result, anyone having access to the application layer doesn't get access to the data layer.
- Within the data layer, Druva encrypts the data using its proprietary envelope encryption technology, making it impossible for anyone besides the customer to access the data.

Access control

One of the most effective ways to protect data is to limit who can access it. If too many people have the ability to access and delete data or reassign administrative roles, threat actors can compromise even low-level credentials and use them to destroy data or lock other administrators out of the backup environment.

We strongly recommend implementing RBAC (Role Based Access Control) to ensure that only a small group of administrators can perform destructive actions like deleting backup data.

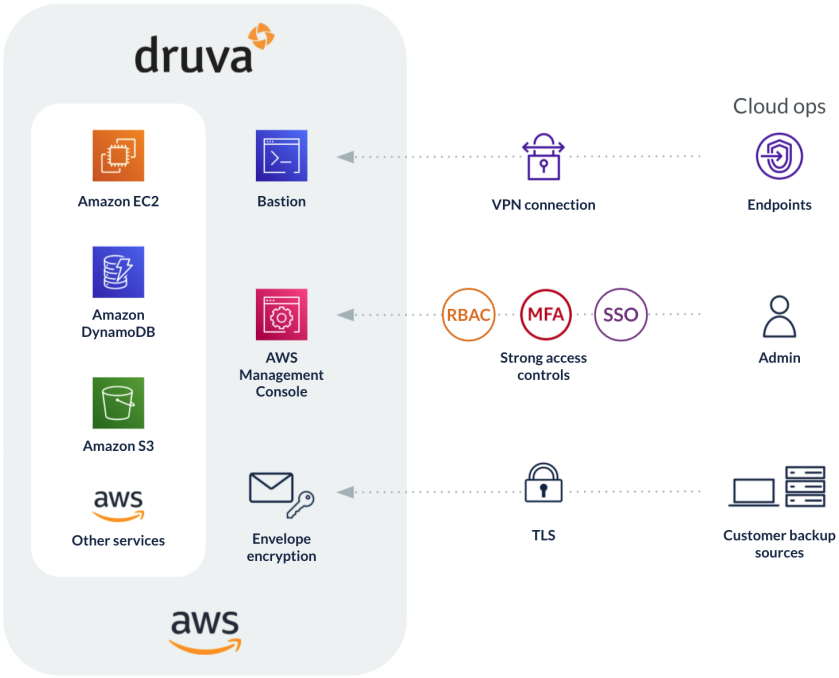
- Administrative control settings prevent end users from deleting backup data. You also have the ability to require two administrators to approve major deletions.
- The Druva platform also provides the ability to customize admin roles to prevent deletion (screenshot below). As a best practice, designate no more than two people in the organization as Druva Admins with the power to delete snapshots.
- Druva's GeoFencing capabilities ensure that access to the backup environment is for known IP addresses blocking out potential attacks from any bad actors or embargoed countries.
- Druva employees cannot access customer data or infrastructure directly, in line with our secure by design philosophy.



Administrator profiles can be created with or without the ability to delete snapshots. We recommend providing no more than two administrators the ability to perform deletions.

It is also important to consider access control for vendor employees. Due to our unique encryption, Druva *never* has access to customer data. We also strictly control how our developers can access the code that powers the Druva Data Resiliency Cloud.

- Access to applications is monitored and controlled via a multi-factor authentication and access control using a combination of Bastion, VPN, MFA and auto expiring dynamic credentials.
- There is no SSH access to production nodes, closing potential security threats from that access point.



Access control is important at all levels. In addition to offering robust access controls to our customers, Druva strictly controls developer access to our own production environment.

Zero-trust security

Access control is only effective if it is difficult to compromise administrative profiles. To prevent threat actors from gaining access to the backup environment using compromised credentials, you can implement zero-trust security protocols.

Zero-trust is a security model based on strict verification processes. This approach treats every access attempt as if it originates from an untrusted source and access is only granted after identity has been verified.

Druva was designed around a zero-trust security architecture and offers rich multi-layered defense features including MFA (Multi-Factor Authentication). Built natively on AWS's security framework, Druva also inherits the global security, compliance and data residency controls, thus adhering to the highest standards for privacy and data security.

2) Operationalize security across primary and backup environments

Selecting a secure backup solution is a good first step toward making your data safe. To truly protect your data, you must build security into the day-to-day operations of your organization. You need to regularly update and patch all your applications, optimize performance, and prevent vulnerabilities.

Typically with an on-premises backup solution, the onus is on the Security Operations or IT administrators to upgrade data protection software and backup appliances on time, as well as apply and maintain security patches to prevent exposure of backups to security threats. Unfortunately, between constrained budgets and a lack of IT resources, many companies fall behind. In fact, 42% of vulnerabilities are exploited after a patch has already been released but not yet applied by IT personnel.

This is why the most successful organizations are turning to SaaS solutions to help them operationalize their security efforts. The software as a service model allows customers to protect their data without the need for extra processes or the cost of additional hardware.

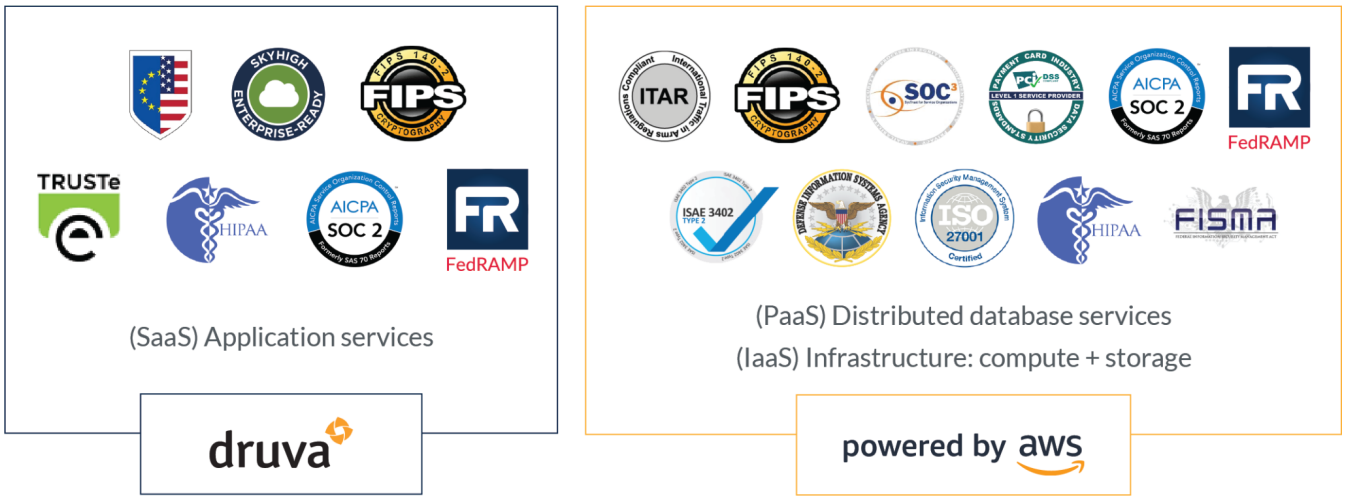
Updates to the Druva Data Resiliency Cloud are completed automatically in the background, eliminating the need to manage timely upgrades or security patches. Additionally, Druva patches known vulnerabilities within 30 days and critical vulnerabilities within the hour — making sure you can stay ahead of ransomware threat actors.

Druva's stringent security compliance and certifications

We're proud of the third-party validation that supports the trustworthiness of our security—one of our core pillars. While many cloud SaaS vendors simply rely on the certifications that the CSPs provide for the infrastructure as their security model, Druva has gone above and beyond, achieving compliance and attestations for our cloud service. To date, Druva is certified or can claim compliance with the following certifications and frameworks, including (but not limited to):

- **SOC 2 type II audited**
- **HIPAA compliance**
- **FIPS 140-2 compliant** (GovCloud environments)
- **FedRAMP moderate ATO** (inSync GovCloud environment)

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



3) Orchestrate response to automatically contain threats

Ransomware attacks almost never occur at 9am on Monday. Instead, threat actors wait until the Friday evening before a three day weekend, or in the middle of a national holiday, when they know most people will be out of the office. You need to be able to respond automatically in the event of a ransomware attack, without the intervention of IT staff.

Your first step should be to quarantine infected resources, in both the primary and backup environments. Stop backing up data from infected machines or servers and prevent anyone from recovering data from affected snapshots. While ransomware cannot execute in the Druva Data Resiliency Cloud, restoring files that contain malicious code can still cause reinfection in the primary environment, taking your recovery process back to square one.

Druva offers built-in API integrations with SOAR (security orchestration automation and response) solutions, such as Palo Alto XSOAR and FireEye Helix, to help automate your ransomware playbook. You can quarantine infected data immediately, without IT intervention.

Stop the spread of ransomware and prevent reinfection with automated ransomware playbooks powered by API integrations with SOAR solutions.

4) Identify anomalous data and activities

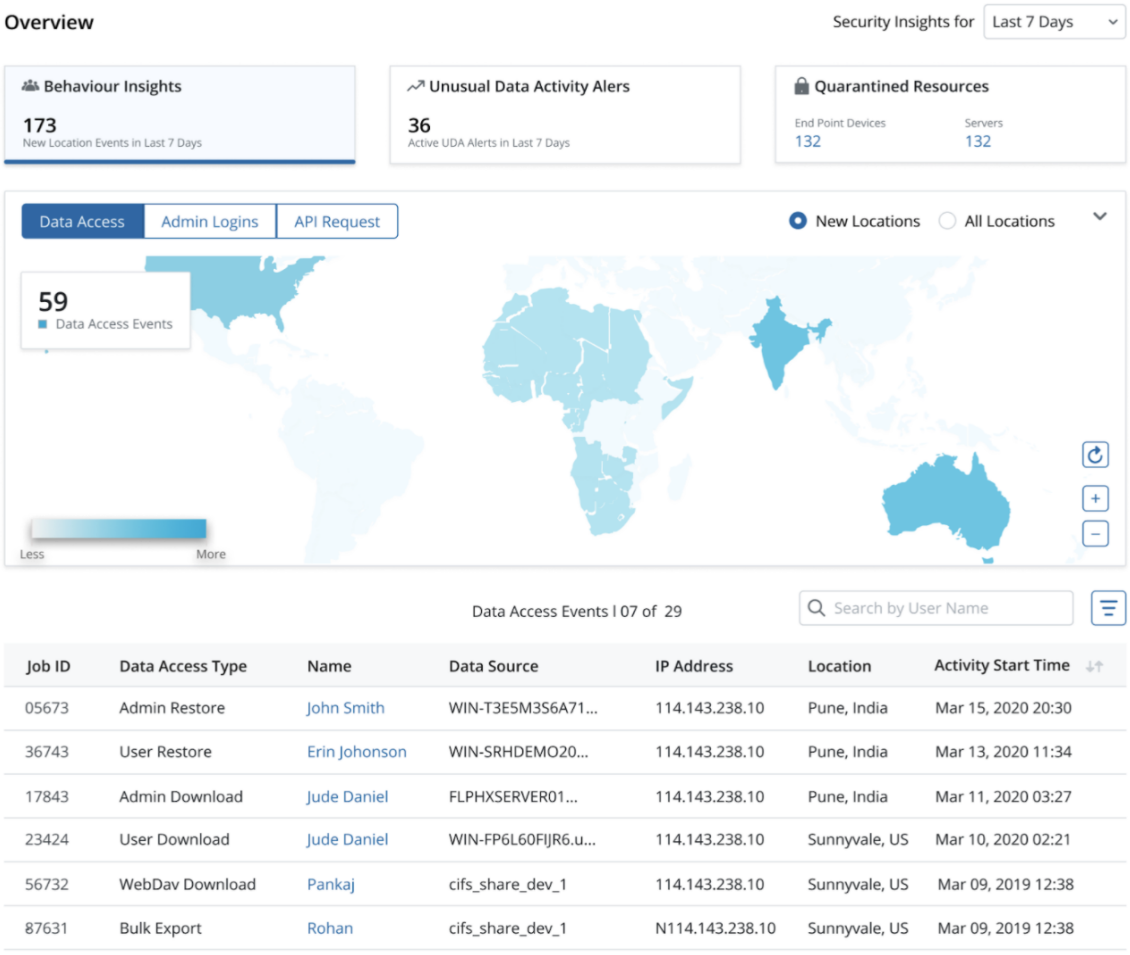
Once you've quarantined affected resources, you need to understand what went wrong during the attack. There are two levels of information that are useful in this process: access insights and unusual data activity.

Access insights

Situational awareness of activity in your backup environment can help you identify malicious actions such as unauthorized access or deletions. The Druva dashboard provides a single pane of glass where you can see all access attempts and activity across all your data sources, including:

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

API integrations can feed this information into SIEM (security information and event management) applications like Splunk and Arcsight for correlation and accelerated incident response.



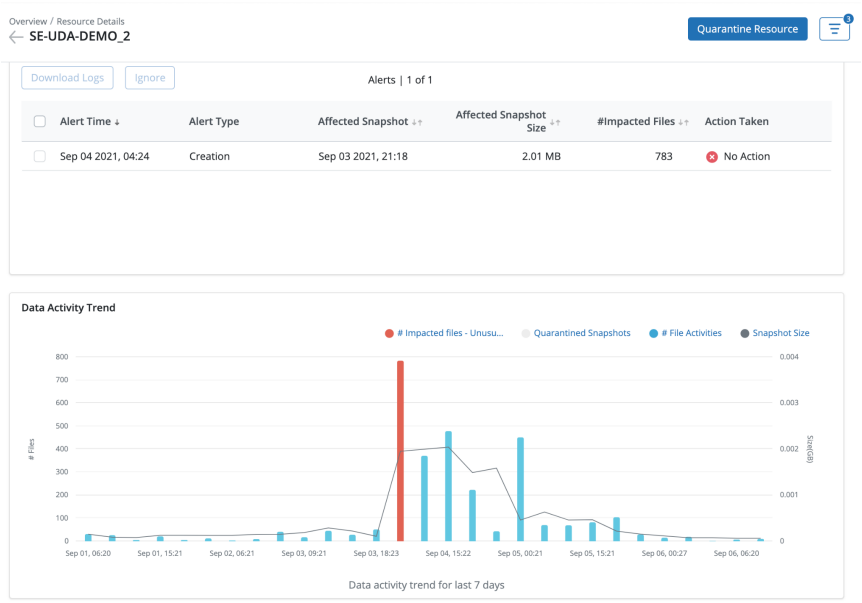
Job ID	Data Access Type	Name	Data Source	IP Address	Location	Activity Start Time
05673	Admin Restore	John Smith	WIN-T3E5M3S6A71...	114.143.238.10	Pune, India	Mar 15, 2020 20:30
36743	User Restore	Erin Johonson	WIN-SRHDEMO20...	114.143.238.10	Pune, India	Mar 13, 2020 11:34
17843	Admin Download	Jude Daniel	FLPHXSERVER01...	114.143.238.10	Pune, India	Mar 11, 2020 03:27
23424	User Download	Jude Daniel	WIN-FP6L60FIJR6.u...	114.143.238.10	Sunnyvale, US	Mar 10, 2020 02:21
56732	WebDav Download	Pankaj	cifs_share_dev_1	114.143.238.10	Sunnyvale, US	Mar 09, 2019 12:38
87631	Bulk Export	Rohan	cifs_share_dev_1	N114.143.238.10	Sunnyvale, US	Mar 09, 2019 12:38

Gain situational awareness in your backup infrastructure using Access Insights to understand access attempts and activity.

Unusual data activity

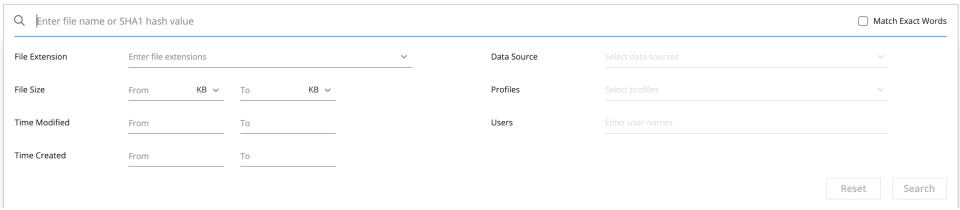
Ransomware attacks also produce anomalies at the data level. Quickly identifying anomalous data sets can help you choose a course of action during the recovery process and even support detection of ransomware attacks.

Druva's Unusual Data Activity feature provides continuous monitoring of your backup data. Our proprietary entropy-based algorithm uses machine learning to understand norms for your specific backup environment and provides automated alerts for unusual data activity including bulk deletion and encryption. You can use these insights to quickly identify affected snapshots during recovery. API integrations also enable you to feed these alerts to your SIEM solution, supporting ransomware detection.



Leverage machine learning to quickly identify anomalous data sets and receive alerts for unusual data activity.

Beyond anomaly detection, Druva's federated search aids forensic investigation teams in identifying which other data sources are infected via a hash and metadata based search, providing more clarity on the scope of a ransomware attack.



Federated search supports forensic investigations with hash and metadata based search.

5) Automate the recovery of complete and clean data

Once you have contained an attack and understand its impact, you are ready to begin the process of actually restoring data. There are several ways in which ransomware recovery is different from standard disaster recovery.

Ransomware attacks are often far reaching and affect more than one type of data or system. Unlike a natural disaster, which destroys data all at once, ransomware encrypts data slowly over time. The average dwell time for ransomware is dropping, but is still over 20 days, making it unlikely that the most recent unencrypted version of each file or dataset will exist within a single snapshot. And with ransomware recovery, you must go through the additional step of ensuring that data is clean before restoring it to your primary environment.

All of these challenges can be addressed with cloud-native infrastructure and automation.

Bulk restore

After an enterprise-wide ransomware attack, it is challenging to recover data across all users and workloads as quickly as possible. For many companies, cost efficiency is also a critical factor. In addition to file or single system recovery, Druva supports bulk recovery of multiple user devices or systems.

- Admin driven and user self serve options to restore end-user data
- Restore to VMs to VPC in the AWS Cloud
- Bulk export for recovering via alternate options like a network share, shipped hard drives, snowball edge

Curated recovery

Druva offers a unique solution to the problem of finding and restoring the most recent unencrypted version of files or data sets after an attack. Until now, IT departments have been forced to restore from a point in time prior to the initial infection, then manually search for more recent versions of individual files. Druva's Curated Recovery feature automates this process, saving time and ensuring you have the most recent unencrypted version of all data.

Now you can simply define the time period of the attack (from initial infection to the present) and let Curated Recovery automatically find the best version of every file. The solution assembles clean versions into a single "golden snapshot" you can use for recovery.

Restoring only clean data

Reinfection is every IT administrator's worst nightmare. Restoring contaminated data can take your whole organization back to square one. That's why it's vital to ensure data is free of malware and IOCs (indicators of compromise) before recovery.

With the Recovery Scans feature, you scan selected snapshots and automatically remove malicious content. You can perform scans using built-in antivirus software, as well as hash values from your own threat intel feeds or forensic investigations. Federated search also allows you to look for compromised data across your entire backup environment.

Once infected data has been identified, admins can delete infected snapshots or files, and wipe-clean infected devices, preventing accidental recovery of contaminated data.

Conclusion

The ransomware threat is becoming more and more critical, and is evolving fast. Legacy backup solutions fail to protect backup data from encryption and deletion, are difficult to maintain, and offer limited response and recovery options. These solutions are also ill-equipped to handle ransomware recovery across workloads that span endpoints, data centers, SaaS applications and the cloud.

You need a sound data protection strategy and a strong data resilience vendor to help you implement and manage it. While ransomware attacks may be inevitable, Druva can ensure your backup data is safe, help you operationalize security across your backup and primary environments, and accelerate the recovery process so you can get back to normal faster.

Contact us for a free trial to check it out yourself: druva.com/free-trial/.

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: +81-3-6890-8667
Singapore: +65 3158-4985
Australia: +61 1300-312-729