druva

White paper

The comprehensive guide to ransomware protection and recovery

The foundation for effective business continuity plan

Q121-20161

Introduction

The rise of ransomware has become a crisis that has crippled organizations world-wide. New strains of ransomware and other malware threats are on the rise, and using more advanced social engineering techniques to facilitate their spread. With more employees transitioning to working remotely, the risks and exposure to ransomware are higher than they have ever been.

Ransomware is a form of malware that encrypts and holds your critical business and customer data hostage, and you are unable to access your data until you pay the demanded "ransom" to obtain the encryption 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, which can permanently shut down your business. With the growing frequency and sophistication of ransomware threats, Security Operations leaders are acutely aware of the consequences of excessive downtime, data loss and business disruption due to ransomware attacks.

In today's diverse and distributed IT environment, restoring the organization's applications and data quickly in the event of a ransomware attack is a significant challenge. According to a December 2019 Gartner analysis of clients' ransomware preparedness, over 90 percent of ransomware attacks are preventable with sound security fundamentals, including an effective backup and recovery strategy. In order to give businesses a framework for adopting a strong cyber resiliency strategy, the National Institute of Standards and Technology (NIST) published the Cyber Security Framework, consisting of guidelines and best practices to manage cybersecurity risk including identification, detection, protection, response and recovery.

Reliable backup and recovery is a crucial line of defense against ransomware. Having secure backup images of critical business data and applications allows companies to roll back in time to recover applications and data before the point of ransomware infection. Organizations should use backup as a defense 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 (formerly known as Office 365).

There are several data protection solutions in the market to help address backup and recovery but on-premises solutions are not immune to ransomware once the data center systems are impacted. Your business needs a solution that provides a comprehensive approach to protecting against ransomware attacks and helping organizations recover with speed/agility and confidence.

5 Steps to protect from and limit the impact of ransomware

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

1. Identify and automate data protection for key business assets
2. Protect backup environment with immutable data
3. Detect early threats potential risks
4. Respond proactively to prevent contamination and threat permeation
5. Recover data quickly with flexible recovery options

1) Identify and automate data protection 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. 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 not only the critical servers and applications that power your business, but also the entry points where ransomware can attack (primarily your end users).

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 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.

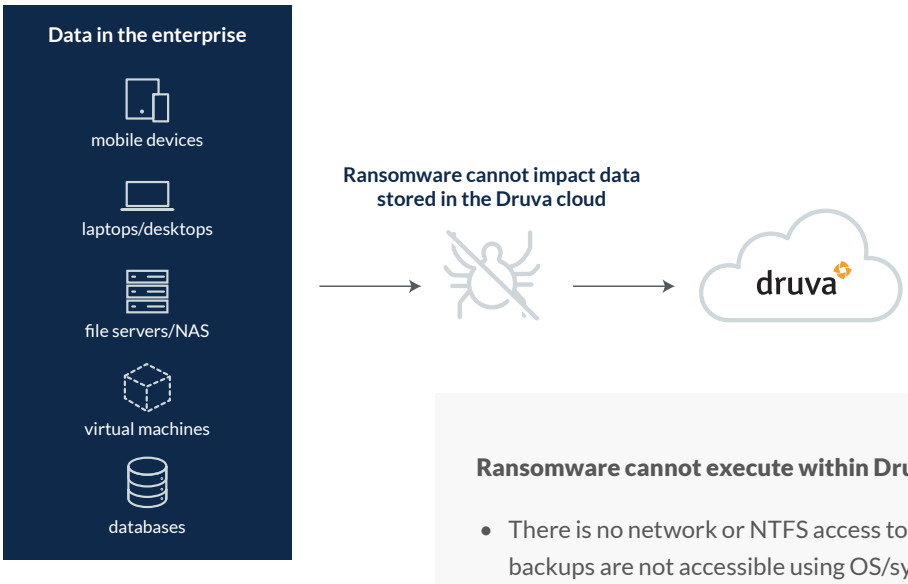
Automating the data protection processes and policies for backing up your key assets ensures that you have up to date backups to facilitate a timely recovery. Configurable backup policies and pre-configured compliance templates assist you with defining the assets to protect, with associated compliance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

Druva offers a unified cloud data protection platform that can protect your endpoints, SaaS applications, data center and AWS workloads, giving you the flexibility to protect all of your key assets.

2) Protect backup environment with immutable data

One of the challenges of on-premises data protection solutions is that they are exposed to the same ransomware threat as the rest of your data center environment. Any backup environment attached to your network can be infected with ransomware, preventing you from accessing your backup data at a critical time.

Unlike an on-premises backup solution, Druva offers built-in, naturally air-gapped and immutable data protection. Backup data is isolated from the customer's infrastructure in the Druva Cloud Platform by design. Ransomware cannot exploit the same threat vectors or security vulnerabilities of the customer's environment to execute itself in Druva's cloud-native backup environment. Druva's cloud-native architecture ensures your backup data is not at risk from ransomware and prevents ransomware from encrypting your clean backup copies.



Ransomware cannot execute within Druva's cloud platform because:

- 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 the 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 direct-attached storage, Active Directory applications, or Remote Desktop Protocol typically used by ransomware.

Data backed-up in the Druva Cloud Platform cannot be modified or deleted by ransomware. Your backup data is protected without the need to manage extra processes or software, or spending additional hardware. It's part of Druva's foundation for the Druva Cloud Platform.

With distributed data and applications, data management, privacy and security has become a ubiquitous challenge for IT teams. 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, security patches applied and regularly maintained to prevent exposure of backups to security threats. Usually, the cost to manage and maintain the on-premises infrastructure and software comes at a price, which could become another challenge given shrinking IT budgets.

Druva was designed around a zero trust security architecture, which is changing the game by enforcing the adoption of newer security best practices to address the security demands on the technology stack and protect your data with a sound defense-in-depth strategy. Built natively on AWS's security framework, Druva inherits the global security, compliance and data residency controls, thus adhering to the highest standards for privacy and data security.

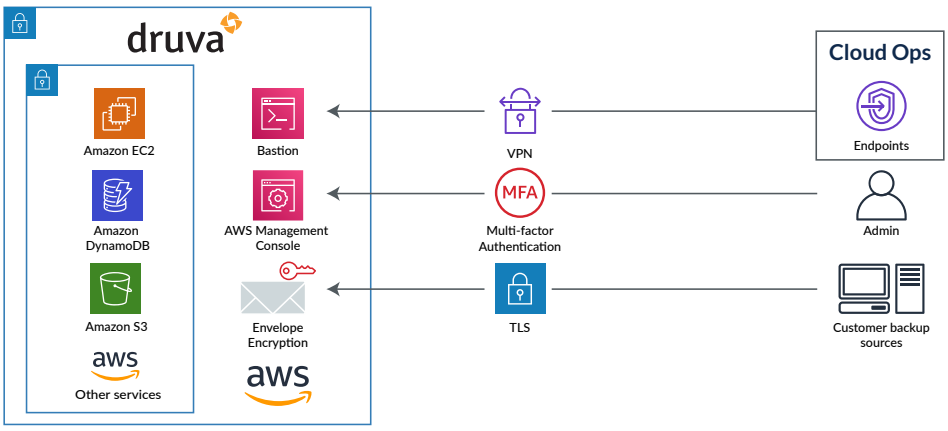
The Druva Cloud Platform is updated frequently to release the latest features and security updates, transparently in the background for our customers. This allows Druva to support continuous feature development and automatically apply new security enhancements without IT needing to manage timely upgrades and maintenance. Any known vulnerabilities patched within 30 days and critical vulnerabilities within the hour - making it always ahead of the game compared to ransomware attackers.

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, security patches applied and regularly maintained to prevent exposure of backups to security threats. Usually, the cost to manage and maintain the on-premises infrastructure and software comes at a price, which could become another challenge given shrinking IT budgets.

Encryption and access control

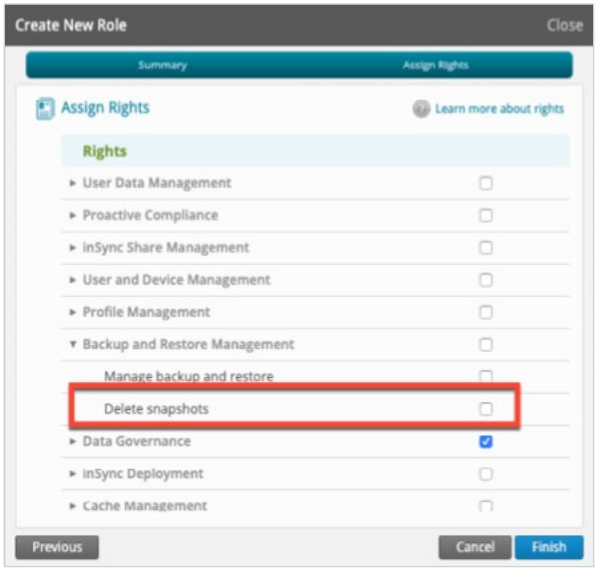
Druva Cloud Platform provides a secure, multi-tenant environment for customer data. Druva issues unique per tenant AES-256 encryption keys and offers encryption for data in flight and at rest. The use of one unique encryption key per customer along with customer held key encryption keys, creates crypto-segmentation between customers, completely avoiding data leakage.

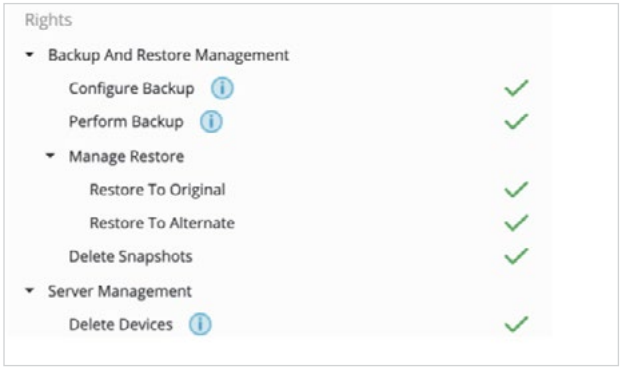
- Druva stores the data by splitting it into blocks and deduplicating, with unique data blocks getting stored into AWS S3 and metadata in AWS DynamoDB and uses AWS EC2 as the computational layer to enable elastic scalability.
- The application layer is separate from the data layer. As a result, anyone 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.
- Druva employees cannot access customer data or infrastructure directly, in line with our secure by design philosophy.



Druva's cloud-native architecture was designed around a zero trust architecture model, with access control being an important aspect of that model beyond the secure method by which we store customer data.

- 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.
- Administrative control settings prevent end users from deleting backup data.
- 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 platform provides the ability to customize admin roles to prevent snapshots deletion (screenshot below). A best practice would be to designate no more than two people in the organization as Druva Admins, and then multiple admins can be created with no rights to delete snapshots.





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.

(SaaS) Application Services

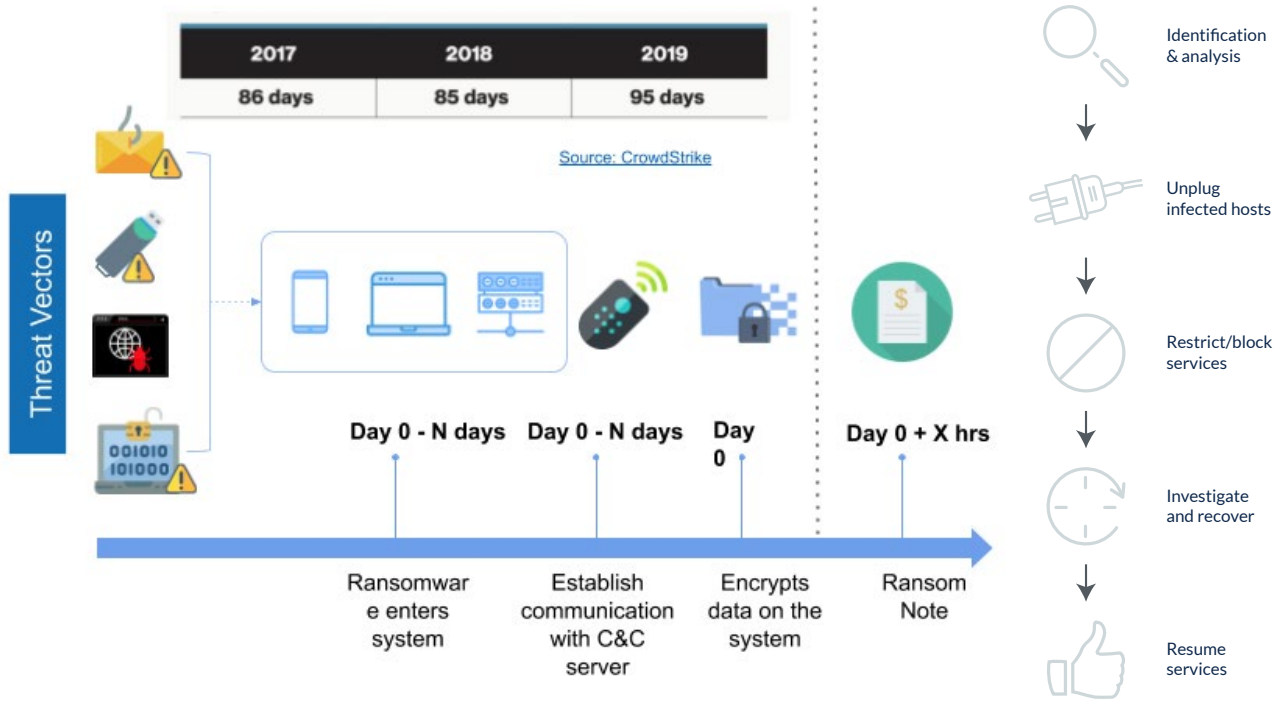
druva

(PaaS) Distributed Database Services
(IaaS) Infrastructure: Compute + Storage

powered by aws

3) Detect early threats potential risks

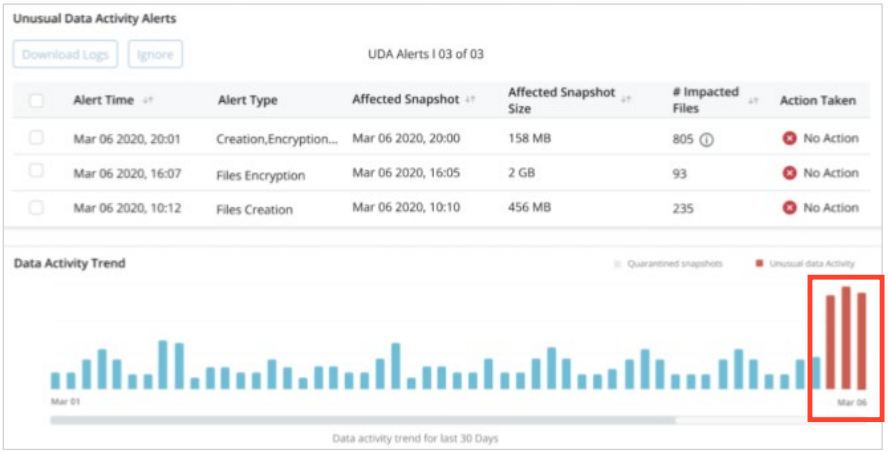
Without proactive monitoring for ransomware threats, the Security Ops team might not be able to detect ransomware until it triggers months after lying dormant inside your data. As per a recent CrowdStrike Global Threat Report, ransomware can sit up to 95 days within the network before proceeding to encrypt critical business data.



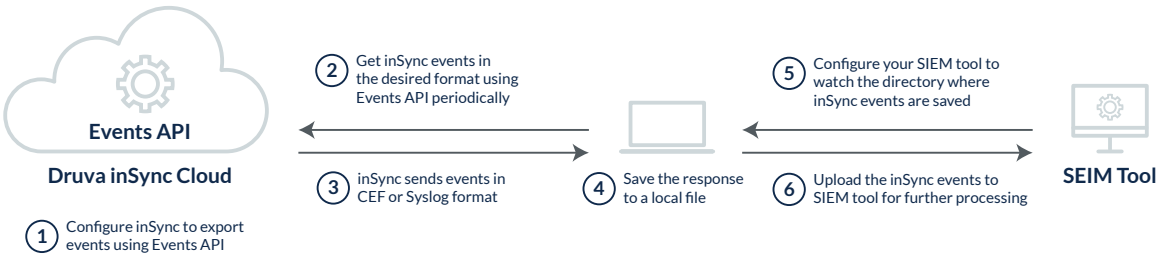
Organizations need to be able to detect any possible threat even if the infected data is in the backup environment. That requires a backup vendor to detect and monitor any potentially infected backup copies, unusual admin and end-user backup and restore activities.

To protect from and monitor for ransomware attacks Druva offers:

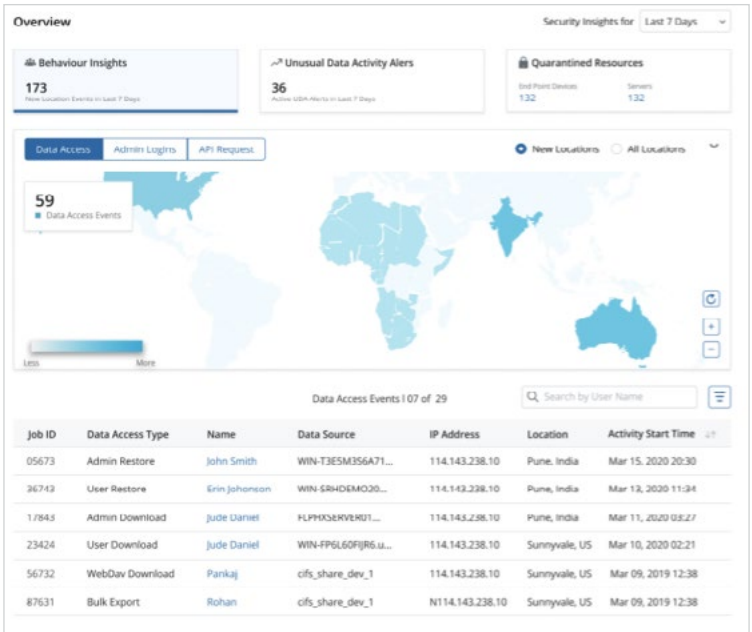
- Complete visibility and automated monitoring to flag potential risks by identifying anomalous data activity using proprietary entropy-based machine learning algorithms based on historical and current change rates.
- Automated alerts and event notifications for potential data anomalies as well as restore, data access, admin policy change activities to give IT admins the visibility the need to make proactive security decisions.



- IT admins can monitor reported failures, detect malicious activity through IP address logging, take corrective actions and capture full audit trail of admin activities. The audit, alerts and events APIs can be integrated into security information and event management applications like Splunk and Arcsight for correlation and accelerated incident response. IT teams can improve productivity and efficiency, being able to manage their backup data within the same analytics environment they are used to for other business processes.



- Druva offers complete visibility and monitoring and identification of anomalous data activity based on historical and current change rates using proprietary entropy-based machine learning algorithms.
- Automatic alerts and event notifications for potential risks around data anomalies non compliance, unusual restores, policy changes and admin activities proactive security decisions.

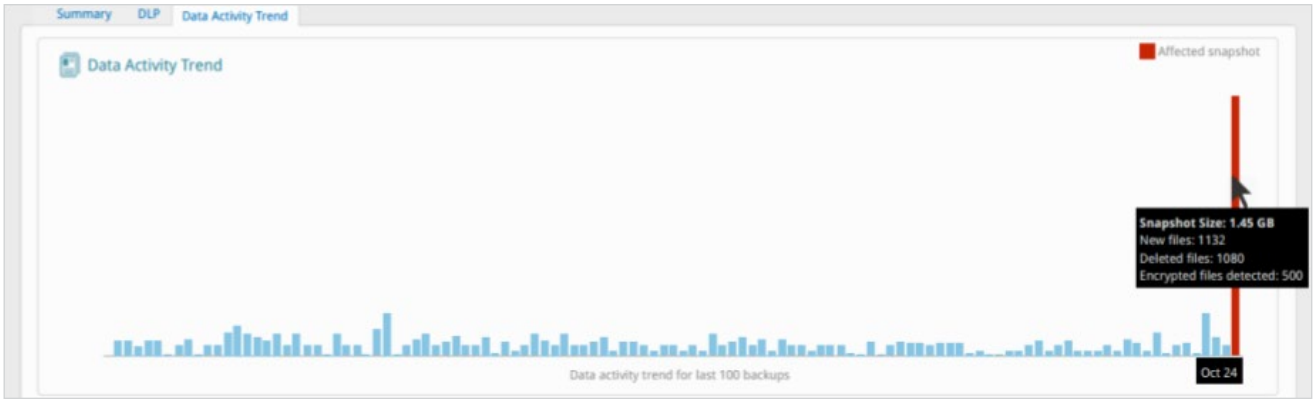


4) Respond proactively to prevent contamination and threat permeation

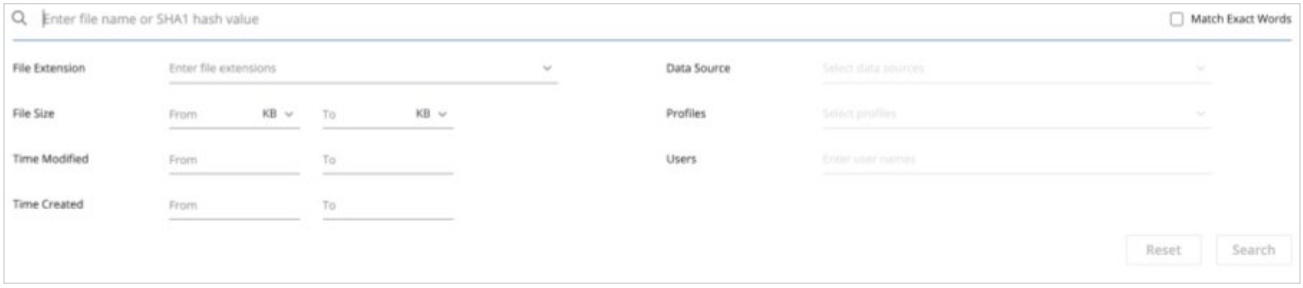
Quickly responding to potential threats is the key to maintaining the safety of your organization's data and applications. Once a threat has been identified, you need the ability to quickly analyze your environment and discover the source of the infection, as well as understand when your data was compromised.

Identify last known good copy

Druva ensures faster identification of the last clean backup or snapshots from infected ones using its anomaly detection capabilities. Druva's proprietary entropy-based machine learning algorithms help identify a clean snapshot to recover from based on historical and current change rates.



Once the last known good copy has been identified, Druva's federated search aids forensic investigation teams in identifying which other data sources are infected via a hash and metadata based search, thus providing more clarity on the scope of a ransomware attack.

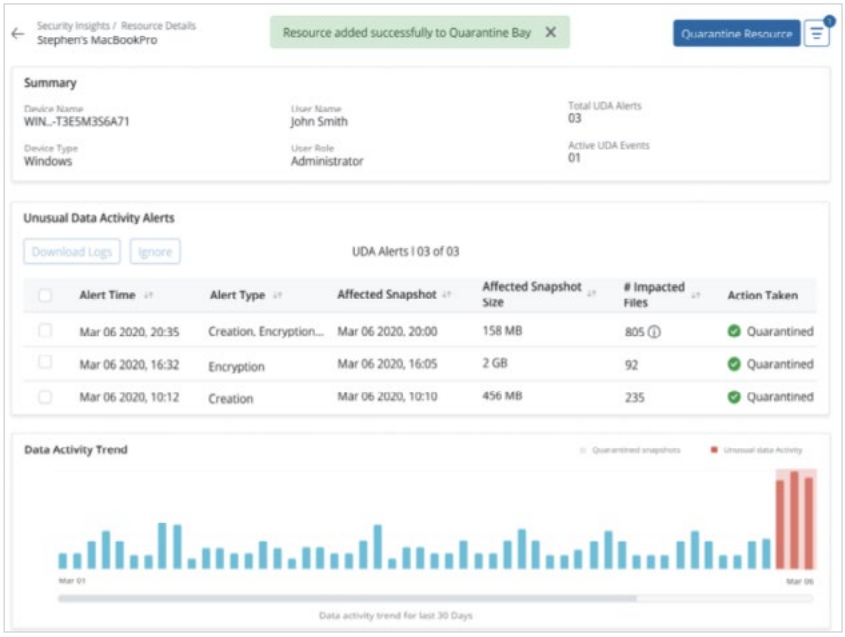


Delete infected snapshots and files

Druva offers multiple features for managing ransomware recovery as well as ensuring the infection is fully removed from the network.

- Admins can delete infected snapshots, thus preventing anyone in the organizations from accidentally recovering data contained within these infected snapshots.
- Admins can wipe-clean a device that has been infected, thus reducing the overall risk exposure from a ransomware attack.

- Druva's federated search offers to search for infected files and indicators of compromise and eliminates these from any backup copies.
- Admins can quarantine or delete infected snapshots based on timestamps or anomalous activity in snapshots.
- Mitigate the enterprise-wide risk of ransomware spread, by blocking restores or downloads of quarantined data from infected snapshots.
- Enable Security Operations teams to orchestrate response actions using API-first capabilities directly via Security Orchestration, Automation & Response (SOAR) applications like Cortex XSOAR from Palo Alto Networks.



5) Recover data quickly with flexible recovery options

The faster your data and applications are recovered, the less of an impact ransomware will have on your organization. However, not every recovery is the same, so having multiple options for how to recover your data is important.

Historic snapshots

Druva provides the ability to recover data from historical snapshots. Admins can set a retention policy for as long as they are comfortable with, to ensure guaranteed recovery with minimal data loss. In case of a ransomware attack, admins can quickly have access to recover data from a date with guidance from their infosec team.

Long term retention of backup data not only protects from ransomware threats, but also helps your business comply with a variety of regulations governing data retention. By storing and retaining this data long term in the cloud, you can reduce your overall storage spend while improving your ability to recover from longer term ransomware infections.

Bulk recovery

The challenge, after an enterprise-wide ransomware attack, is to recover data across all users and workloads in the fastest possible way and for many companies, cost efficiency is a critical factor. In addition to file or single system recovery, Druva today supports various options for bulk recovery of multiple user devices or systems

- Admin driven and user self serve options to restore end-user data
- Mass deployment support for bulk redeployment
- 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
- Identification of safe snapshots to restore from and recover with confidence

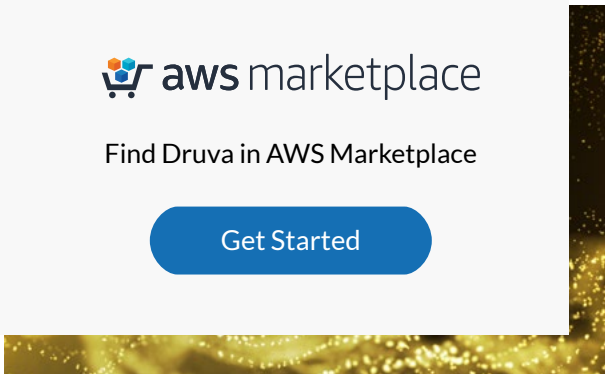
Conclusion

The ransomware threat is becoming more and more critical, and is evolving fast. Current infrastructures just can't identify or recover from ransomware fast enough, especially across workloads that span endpoints, data center, SaaS applications and the cloud. The existing solutions available have security risks and need to be immune themselves first to protect the customer from ransomware.

You need a sound data protection strategy and a vendor like Druva to help you through your business resiliency and continuity journey along with effective employee education. While no backup vendor can immunize you from future malware attacks, Druva can guarantee that you can significantly increase your odds of faster response and recovery.

Druva's comprehensive cloud data protection and robust defense-in-depth security and compliant platform can power Security Operations and IT teams to protect, detect, respond and recover faster in case of any external or internal attacks, ransomware, insider attacks, accidental or malicious data deletion.

Now that you know how Druva can help, you can contact us for a free trial to check it out yourself:
www.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

Druva™ delivers data protection and management for the cloud era. Druva Cloud Platform is built on AWS and offered as-a-Service; customers drive down costs by up to 50 percent by freeing themselves from the burden of unnecessary hardware, capacity planning, and software management. Druva is trusted worldwide by over 4,000 companies at the forefront of embracing cloud. Druva is a privately held company headquartered in Sunnyvale, California and is funded by Sequoia Capital, Tenaya Capital, Riverwood Capital, Viking Global Investors, and Nexus Partners. Visit Druva and follow us @druvainc.