druva

Solution brief

Ransomware Protection and Recovery with Druva

Recover from ransomware in hours, not days

The challenge

Ransomware is a relentless threat to every enterprise, with attacks expected to occur every 2 seconds by 2031, up from every 11 seconds in 2021.[1] The damage can be catastrophic: 93% of companies that lost their data for 10 days or more filed for bankruptcy within one year of the disaster, and 50% filed for bankruptcy immediately.[2]

Ransomware attacks are not only happening more frequently but becoming more technologically advanced and expensive. The average ransomware payment demand was $228,125 in Q2 2022 (up 8% from Q1 2022).[3] An increasing number of ransomware attacks involve the deletion of backup data, providing a strong incentive to pay.

The financial impacts above don't take into account the additional costs associated with lost productivity or reputation damages. A 2022 report found that the average downtime from a ransomware attack reached 26 days.[4]

The solution

Druva Data Resiliency Cloud simplifies and accelerates the complex process of responding to and recovering from ransomware. A foundational protection layer ensures both data integrity and availability of backup data with no hardware or overhead. Because rapid response requires preparation and cyber recovery requires automation, Druva built the critical capabilities needed to address these needs.

Druva Cyber Resiliency and Ransomware Protection

Protect

Data Integrity & Availability

Operational Security

It's simple to keep your backup data safe. No hardware, software, manual updates, or complex configurations.

Prepare

Posture & Observability

Continuous Monitoring

Get a centralized view of all your security posture and data risks so you can be ready for cyber attacks.

Recover

Accelerated Recovery

Forensics

Automate the process of recovering clean and complete data sets so you can get back to normal.

API integrations with security solutions

paloalto NETWORKS Trellix splunk>

Trust Certifications

FedRAMP FIPS 140-2 CRYPTOGRAPHY AICPA SOC 2 SKYHIGH ENTERPRISE-READY TRUSTe

Protect

The first step in preventing damage from ransomware is ensuring that you have a clean and available backup copy of your data. In order to access this data quickly, you need both your backup platform and data to be highly available and secure. Built on the highly resilient AWS infrastructure, Druva provides both data integrity and availability. A zero trust architecture provides the foundation for operational security managed by the Druva Cloud and Security Operations Teams. Druva makes it impossible for ransomware to encrypt backup data (air-gapped backups, separate data and metadata objects, and data sharding). Should a malicious insider or bad actor bulk delete backups, Druva will alert you and enable roll-back of deleted backup data. Druva provides foundational security for all you critical data sources - endpoints, data center, cloud, and SaaS apps - with no additional overhead:

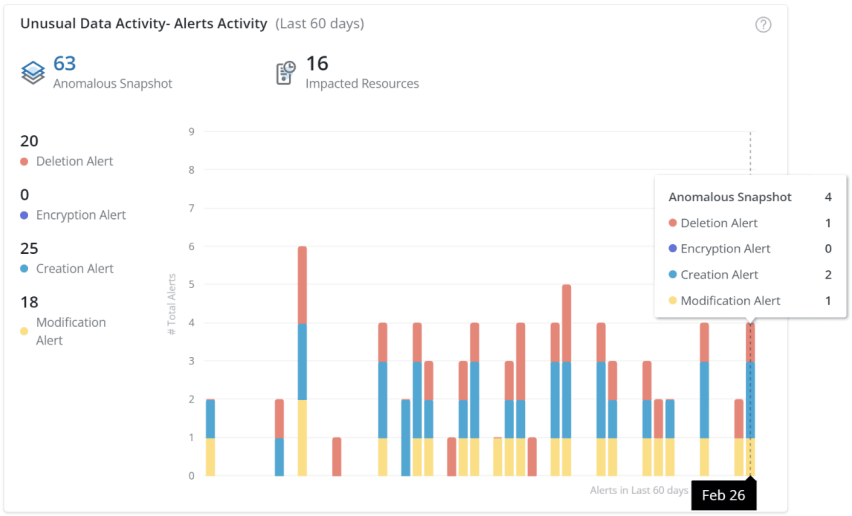
- **Built-in data security:** Air-gapped backups, envelope encryption, Druva Data Lock for immutability, and bulk deletion monitoring
- **Multi-layer access controls:** Built-in multi-factor authentication(MFA), SSO integration, and separate account access (to ensure that ransomware actors cannot use compromised primary environment credentials to tamper with backup data)
- **Operational platform security:** Vulnerability scanning, automatic patching and upgrades

Druva Data Lock allows organizations to create immutable, tamper-proof backups (and policies), to meet compliance and security needs. Data Lock prevents any changes to backups by any administrator and sends alert notifications and emails when anyone attempts to modify policy settings.

Prepare

Ensure attack readiness with Druva. Your backup data mirrors your primary environment and is a rich source of information. IT and security teams can be better prepared to respond to security incidents with Druva's Security Posture and Observability solution. It provides continuous security posture monitoring, access insights, and anomaly detection across backup data. Leverage native alerts and reporting or integrate with your security stack (i.e., SIEM) using pre-built integrations or Druva APIs.

- **Understand your data security posture:** Receive a real-time security posture risk assessment and in-depth insights into your Druva cloud platform security, data compliance, data protection reliability, and data access patterns.
- **Enhance anomaly detection:** Automate detection of security events and data anomalies such as unusual restore requests, file additions or data encryption using Druva's proprietary machine learning (ML) algorithms that require no rules setup or tuning.
- **Detect and rollback deletions:** Monitor and recover from accidental or malicious deletions of business critical data



Anomaly detection alert summary showing unusual data activity (UDA)

Respond and Recover

Once you've detected an attack, rapid response is vital to ensure a fast recovery. There are many valuable primary environment security tools that can be used for detection and orchestrated response. Druva's Accelerated Ransomware Recovery Solution can dramatically reduce the mean time to respond (MTTR) and recover by automating actions like quarantine infected systems or snapshots, providing access to critical log data, accelerating recovery of clean data with curated snapshots, and built-in malware scanning.

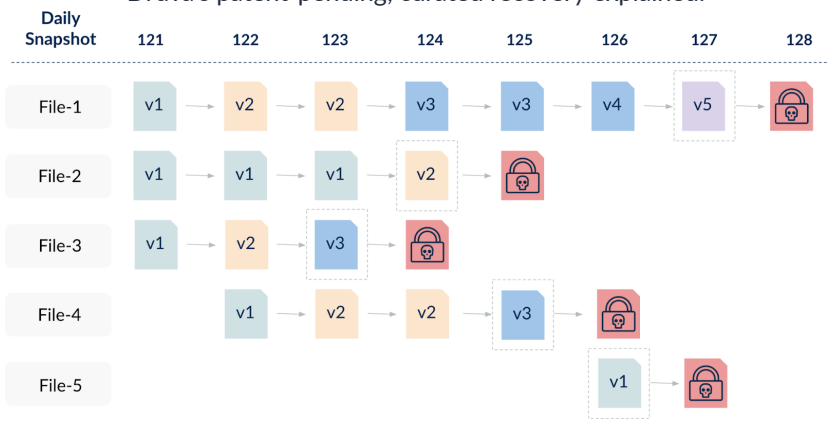
Cyber recovery is different and harder than traditional business continuity or disaster recovery scenarios because trust has been broken across the enterprise IT environment. For most companies, recovery is a manual and time-consuming process. With average dwell time of ransomware attackers at 10 days[5], it can be difficult to identify the best backup snapshot to use for recovery. Even after the best snapshot is identified, hidden malware can cause reinfection. Plus, if data is recovered from a point too far in the past, you'll need to manually find and recover clean versions of important files that were created or modified in the intervening time.

Druva Accelerated Ransomware Recovery solution enables you to respond and recover with confidence and speed while ensuring the hygiene of recovered data.

- **Accelerate investigations** with rapid access to logs and anomalies across data sets, users, and locations. Support forensics by searching endpoint backup data for malicious hashes.
- **Quarantine backups at scale** to prevent reinfection.
- **Delete infected snapshots** and files across endpoint backups.
- **Filter out malware** with recovery scans using known or custom IOCs.
- **Find the most recent clean data fast** with curated recovery by automatically finding the best possible file across multiple snapshots at scale to reduce data loss.
- **Automate response and recovery actions** with pre-packed integrations for SOAR tools or build your own automated ransomware playbooks using Druva APIs.

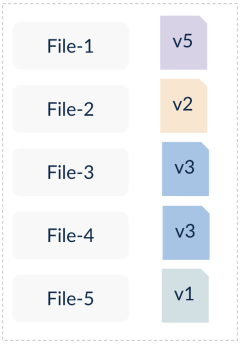
Save time and reduce data loss with automation

Druva's patent-pending, curated recovery explained.



Curated Recovery

Automatically finds the most recent clean version of each file and adds it to a single "curated snapshot"



With the Druva Data Resiliency Cloud, you get guaranteed resilience, protection without backup infrastructure headaches, insights to prepare for an attack, and the automation to respond and recover quickly and safely.

For more information

druva.com/use-cases/ransomware

1. "Ransomware Will Strike Every 2 Seconds By 2031," Cybersecurity Ventures, Steven Morgan, 13 Sep 2022
2. National Archives & Records Administration
3. "Ransomware median falls in Q2 2022," Coveware, 28 Jul 2022
4. "Ransomware Threat Actors Pivot from Big Game to Big Shame Hunting," Coveware, 25 May 2022
5. The State of Ransomware 2023, Sophos, May 2023

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.