Accelerated Ransomware Recovery

Shorten incident response time and cyberattack recovery with automated security workflows and integrations

The challenge

Recovering clean data quickly after a ransomware attack is problematic and challenging for most organizations. The common and misplaced assumption is that "data recovery" is the same for all use cases be it a cyber incident or disaster recovery (DR scenario). It is not. In a DR scenario, you presume data integrity, but with ransomware, you presume data compromise which requires cross-team collaboration, shared tools, and automation. IDC found that over 50% of organizations worldwide have been impacted by ransomware, yet only 32% could fully recover data without paying a ransom.

Our perspective

A good backup copy is only the first step to recovery when data integrity is compromised due to a cyber attack. IT teams can collaborate with security teams to accelerate response, forensics, and recovery efforts when they have guaranteed access to clean backup data and logs as well as automation for both ransomware recovery playbooks and SOAR tools. With a cloud-based platform, these teams can quickly quarantine suspect snapshots, scan data before restore and automatically minimize data loss across multiple recovery points.

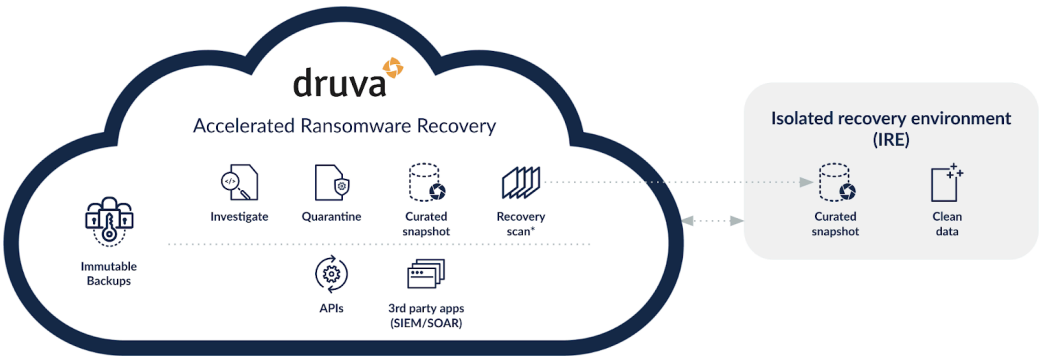
The Druva Data Security Cloud provides a foundational protection layer that ensures both data integrity and availability with air-gapped, immutable backups. In addition, Druva's Managed Data Detection and Response service provides 24/7 expert monitoring of your backup environment. Once we verify a threat, our team works with you to secure and roll back to clean data, preventing data loss and downtime.

Develop an operational runbook for cyber attack recovery

Recovery from ransomware is different. Druva improves how you prepare, respond, and recover with prebuilt workflows focused on ransomware threat investigation, response, and recovery.

Key ransomware investigation and recovery needs

- **Investigation** — Accelerate efforts with rapid access to logs and anomalies across data sets, users, and locations
- **Quarantine** — Automate quarantine of backups at scale to prevent accidental reinfection
- **Recovery** — Filter out malware during recovery using known or custom IOCs to prevent re-infection
- **Data loss** — Leverage curated recovery to find the best possible recovery point across multiple snapshots at scale



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

Key features

- **Threat Hunting** — Leveraging advanced analytics and backup telemetry, search, contain, and eliminate threats to your backup environment. Search based on metadata to locate infections and quarantine malicious files prior to recovery to prevent reinfection. Finally, via defensible deletion, ensure compromised files are permanently removed.
- **Recovery Scans** — Filter out malware based on AV scans and augment with custom file indicators of compromise.
- **Quarantine** — Quarantine backups at the snapshot, device, and VM level quickly and easily within the Druva console or leverage third-party integrations and Druva APIs to automate the quarantine process.
- **Curated Recovery** — Infections happen over days or weeks making traditional granular recovery across snapshots tedious or subject to data loss as your team chooses a recovery point date prior to the first infection. Curated Recovery eliminates this problem and allows you to minimize data loss at scale using the power of our cloud. Druva builds curated snapshots by searching across an incident timeline, using algorithmic data analysis, to find the most recent versions of clean files.
- **APIs & SOAR Integrations** — Accelerate time to value with pre-packaged integrations for security, orchestration, automation, and response (SOAR) tools such as Palo Alto Networks Cortex™ XSOAR. Or build your own automated playbooks using Druva APIs. Automate response actions like quarantining to stop the spread of ransomware or prevent re-infection. Support forensics by searching backup data for malicious hashes to accelerate remediation. Automate recovery at-scale, restoring data to a point prior to an attack or by remotely wiping an infected system.

Accelerated ransomware recovery requires far more than instant recovery. With the Druva Data Security Cloud, you get guaranteed resilience, protection without backup infrastructure headaches, insights to help you prepare for an attack, and the automation to recover quickly and safely.

What our customers are saying

"With Druva and the counsel it provided, it was easy to just log in and do the restore. After we wiped the affected endpoint, we fully restored the affected data from the Druva backup in a couple of minutes."

vertrax

Rob Ljunggren
Director of IT
Learn more in the case study

"This was our first time getting attacked like this and we needed outside help." The firm recovered 100% of its data protected by Druva.

Billion Dollar Construction Firm
Senior IT Leader
Learn more in the case study

aws marketplace

Find Druva in AWS Marketplace

Get started

AWS Marketplace is a digital catalog of third-party software, services, and data that makes it easy to find, buy, deploy, and manage software on AWS.

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

Druva, the autonomous data security company, puts data security on autopilot with a 100% SaaS, fully managed platform to secure and recover data from all threats. The Druva Data Security Cloud ensures the availability, confidentiality, and fidelity of data, and provides customers with autonomous protection, rapid incident response, and guaranteed data recovery. The company is trusted by its more than 6,000 customers, including 65 of the Fortune 500, to defend business data in today's ever-connected world. Amidst a rapidly evolving security landscape, Druva offers a $10 million Data Resiliency Guarantee ensuring customer data is protected and secure against every cyber threat. Visit druva.com and follow us on LinkedIn, Twitter, and Facebook.