druva

Ransomware Protection and Recovery with Druva

Recover from ransomware in hours, not days.

The challenge

With attacks expected to occur every 2 seconds by 2031, up from every 11 seconds in 2021,[1] ransomware has proven to be a persistent and evolving threat. Cyber incidents are happening more frequently and becoming more technologically advanced and costly. The average ransomware payment demand was $228,125 in Q2 2022 (up 8% from Q1 2022).[2] The fiscal impacts go beyond a ransom payment with additional costs associated with lost productivity or reputational damage. A 2022 report found that the average downtime from a ransomware attack reached 26 days.[3] 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.[4] Tactics have grown beyond encryption and exfiltration with an increasing number of ransomware attacks targeting backups, creating a stronger incentive to pay.

The solution

Druva Data Security Cloud simplifies and accelerates the complex process of responding to and recovering from ransomware. A foundational protection layer ensures both the data integrity and availability of backup data with no hardware, maintenance, or overhead. Druva built the critical capabilities needed to rapidly respond and successfully recover from a cyber incident and guarantees the security, immutability, and availability of your data up to $10M with an industry-leading Data Resiliency Guarantee. Druva's DRG protects against 5 key threat areas: cyber, human, application, operational, and environmental risks.

Druva's cyber resiliency and ransomware protection

Autonomous protection		Rapid response		Guaranteed recovery	
Automated data protection	**Foundational security**	**Security posture**	**Continuous monitoring**	**Accelerated recovery**	**Forensics**
No hardware, software, manual updates, or complex configurations to keep your backup data secure. Druva does it all for you.		Continuous monitoring with a centralized view of your security posture and data risks so you can quickly respond to threats.		Automate the process of recovering clean and complete data sets so you can get back to business and avoid reinfection.	

API integrations with security solutions

paloalto NETWORKS   Trellix   splunk>

Trust certifications

FedRAMP   FIPS 140-2 CRYPTOGRAPHIC   AICPA SOC 2   (EU/US)   SKYHIGH ENTERPRISE-READY   TRUSTe

Autonomous protection

With a zero-trust architecture, Druva provides the foundation for operational security managed by the Druva Cloud and Security Operations Teams. Druva continually provides up-to-date security patching and around-the-clock cloud operations, and utilizes cloud services with a minimal attack surface, like AWS lambda, with no OS to patch.

Druva makes it impossible for ransomware to encrypt backup data via air-gapped backups. Additionally, data is stored securely based on design principles of dual envelope encryption, data chunking, and data/ metadata separation. Druva provides foundational security for all of your 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, RBAC, and separate account access to backups.

- **Operational platform security:** Vulnerability scanning, automatic patching, and upgrades.

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

Rapid response

Your backup data mirrors your primary environment and is a centralized repository of critical business information that can be exploited by bad actors. Druva provides real-time visibility into the security posture of your sensitive backup data that can be integrated into your security operations. Additionally, Druva's deep data layer observability can be leveraged by backup and security teams to quickly investigate and recover from incidents. These capabilities are complementary to traditional prevention and detection security tools. IT and Security teams can leverage these capabilities via the Druva console, open APIs and pre-built integrations into security tools (e.g., SIEM, SOAR).

- **Understand your data security posture:** Get real-time security posture risk assessment and in-depth insights into your Druva cloud platform's security, compliance, data protection, reliability, and data access patterns.

- **Enhanced anomaly detection:** Automate detection of access 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, continuously drawing from Druva's global SaaS data telemetry.

- **Deletions: detect and roll back:** Monitor and recover from accidental or malicious deletions of business-critical data.
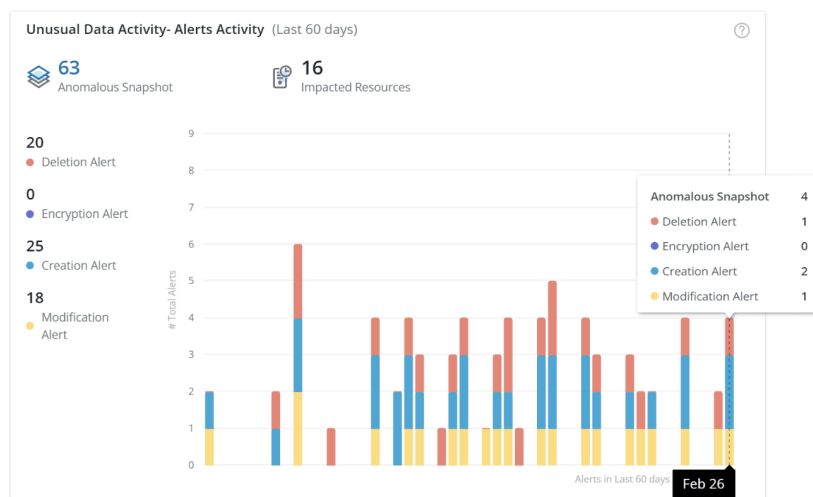
Anomaly detection alert summary showing data anomalies

Guaranteed recovery

Your ability to rapidly respond has a direct correlation to successfully recovering from a ransomware attack. Druva reduces the time it takes to recover by providing additional cyber recovery capabilities that help customers minimize data loss, recover data safely, and prevent reinfection.

Cyber recovery is different and arguably more challenging 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 the 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 efforts to recover clean data, hidden malware can cause reinfection. And 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 enables you to respond and recover with confidence and speed while ensuring the hygiene of recovered data.

- **Find the most recent clean data fast:** Curate recovery by automatically finding the best possible file across multiple snapshots at scale to reduce data loss.
- **Delete infected snapshots:** Quickly locate and remove compromised files across endpoint backups.
- **Filter out malware:** Scan for recovery using known or custom IOCs.
- **Quarantine backups at scale:** Prevent reinfection.

Save time and reduce data loss with automation

Druva's patent-pending, curated recovery explained
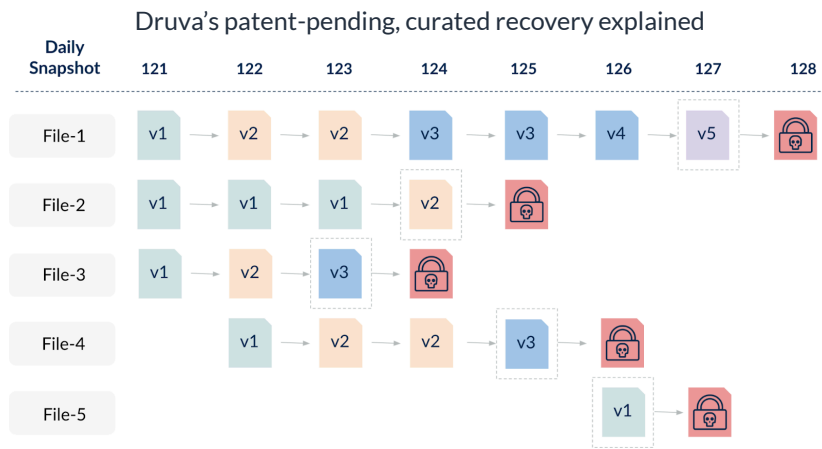
Curated Recovery

Automatically finds the most recent clean version of each file and adds it to a single "curated snapshot"
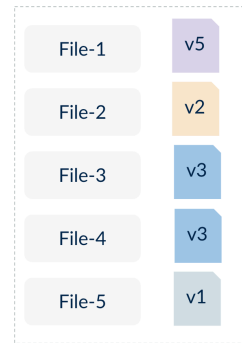
Backed by the Druva Data Resiliency Guarantee and our industry-leading observability and cyber recovery features, Druva provides you with the assurance to be ready for ransomware incidents and recover in a rapid, safe and accurate manner.

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 JulyJul 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