Ransomware Protection and Recovery with Druva

Recover from ransomware in hours, not days

The challenge

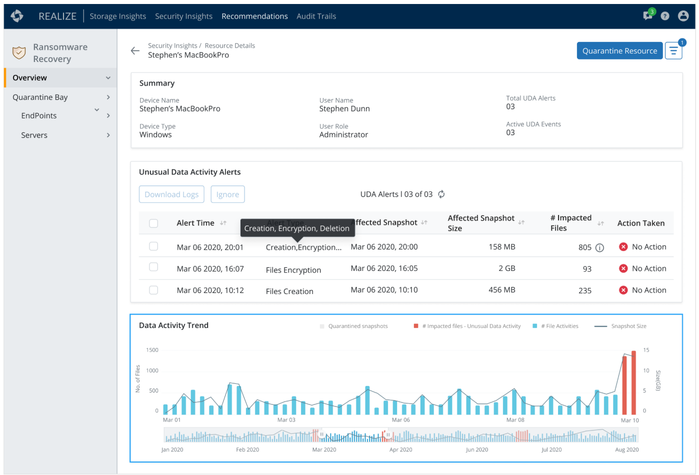
Ransomware is a relentless threat to every enterprise, with attacks expected to occur every 2 seconds by 2031, up from every 11 seconds in 2021.[1] The damage can be catastrophic: 93% of companies that lost their data for 10 days or more filed for bankruptcy within one year of the disaster, and 50% filed 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 and reputational damages. A 2022 report found that the average downtime from a ransomware attack reached 26 days.[4]

The solution

Fast, reliable data recovery eliminates any reason to even think of paying a ransom. When pristine, air-gapped snapshots of workloads and VMs can be restored in minutes, you can transform ransomware into a minor nuisance instead of a devastating ordeal.



Security Insights / Resource Details
Stephen's MacBookPro

Summary

Device Name Stephen's MacBookPro	User Name Stephen Dunn	Total UDA Alerts 03
Device Type Windows	User Role Administrator	Active UDA Events 03

Unusual Data Activity Alerts

UDA Alerts I 03 of 03

□	Alert Time	Alert Type	Affected Snapshot	Affected Snapshot Size	# Impacted Files	Action Taken
□	Mar 06 2020, 20:01	Creation,Encryption...	Mar 06 2020, 20:00	158 MB	805	☒ No Action
□	Mar 06 2020, 16:07	Files Encryption	Mar 06 2020, 16:05	2 GB	93	☒ No Action
□	Mar 06 2020, 10:12	Files Creation	Mar 06 2020, 10:10	456 MB	235	☒ No Action

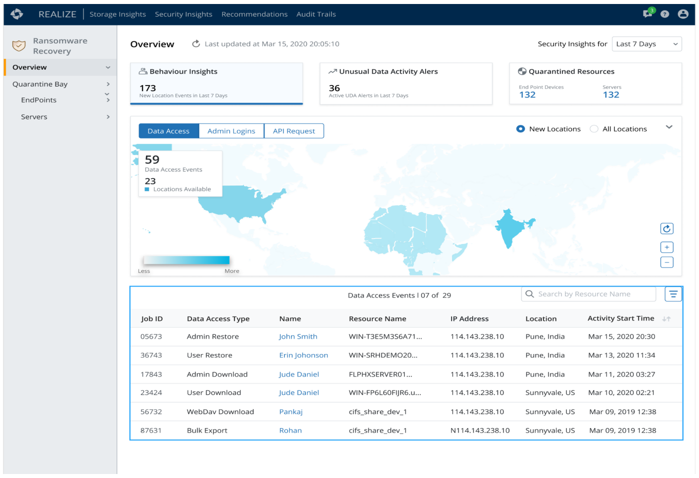
Creation, Encryption, Deletion

Business challenges

- Ransomware attacks that are more frequent, advanced, and expensive
- Inability to quickly identify and restore uninfected backups or files
- Contamination spread and reinfected from recovery data
- Data loss, inability recover a complete data set
- Difficulties coordinating incident response orchestration
- Demands for faster RPO/RTO times
- Costly business downtime leading to loss of revenue and damage to brand reputation
- Legal and regulatory fines from inadequate data protection

Key capabilities

- For all workloads:
  - Ensure you always have clean backup data to restore from in the event of an attack
  - Recover on-premises or in the cloud with RPO/RTO of hours, not days or weeks
  - Restore workloads and VMs across any AWS region/account
- Accelerated Ransomware Recovery for endpoints, file servers, and NAS:
  - Monitor and proactively detect anomalies with ML-based algorithms
  - Orchestrate response and recovery activities via built-in SIEM and SOAR integrations
  - Scan snapshots for malware and IOCs before recovery with Druva or custom file IOCs
  - Delete infected snapshots and files on all endpoint backups
  - Automatically recover the most recent clean version of every file in a specified timeframe



Data Access Events I 07 of 29

Job ID	Data Access Type	Name	Resource Name	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 insight into access requests and receive alerts for anomalous data activity.

Protection

The first step in preventing damage from ransomware is ensuring that you have a clean backup copy of your data. Built on the highly resilient AWS S3 cloud, the structure of Druva's cloud backups makes it impossible for ransomware to encrypt backup data. Zero trust architecture, including multi-factor authentication, envelope encryption, and separate account access ensures that ransomware cannot use compromised primary environment credentials to tamper with backup data. Finally, excess deletion prevention and soft-delete (recycle bin) features provide a further layer of security to safeguard backups against deletion.

Detection

Detecting a ransomware attack as soon as possible can help prevent contamination spread. Druva's Accelerated Ransomware Recovery module provides access insights and anomaly detection that help you quickly identify possible ransomware attacks. Access insights let you see location, identity, and activity information for all access attempts. Anomaly detection uses Druva's proprietary machine learning (ML) algorithms to provide alerts for unusual data activity. The algorithm learns the norms for your specific backup environment so it doesn't require any rules setup or tuning. It also uses entropy-based insights to reduce false positives.

Response

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 orchestration. Druva's Accelerated Ransomware Recovery module offers robust API integrations out of the box that make it easy to fit the solution into your overall security ecosystem. Orchestrating response activities using SIEM and SOAR solutions can dramatically reduce your mean time to respond (MTTR) by automatically completing actions like quarantining infected systems or snapshots based on a predetermined ransomware playbook.

Recovery

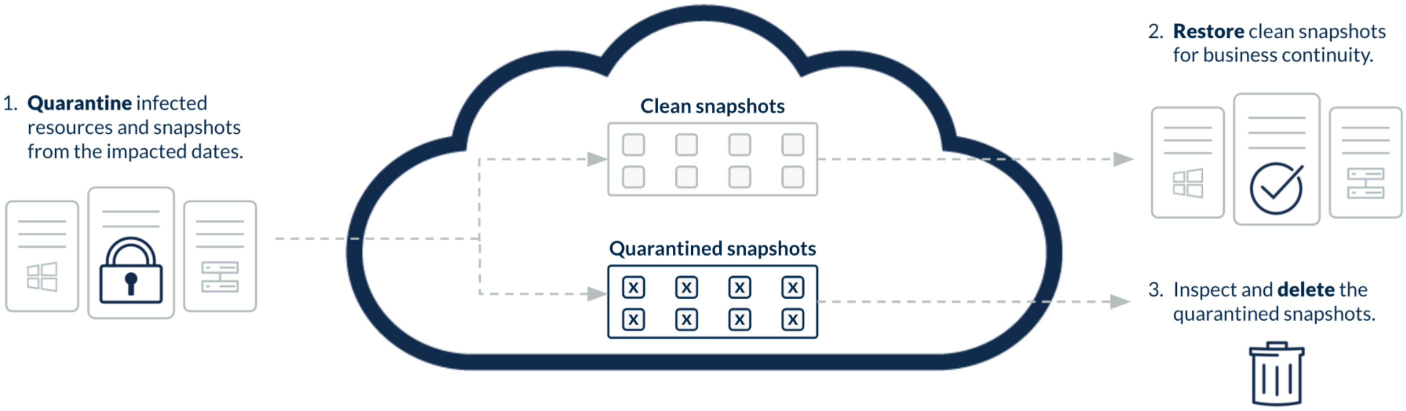
After the initial response phase comes the hard work of recovery. For many companies, this is a manual and time-consuming process. On average, ransomware quietly spreads within a system for 90 days before an actual ransom demand, so it can be difficult to identify the best backup snapshot to use for recovery. Even after the best snapshot is identified, hidden malware can cause reinfection. Plus, if data is recovered from a point in time weeks or even months 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 eases this burden with effective backup architecture and automated tools to accelerate recovery. The Druva Cloud Platform backs up workloads directly to Druva's cloud, ready for immediate recovery in the event of a ransomware attack.

The Accelerated Ransomware Recovery module enables you to recover with confidence by ensuring the hygiene of recovery data. You can scan snapshots for malware and IOCs using built-in antivirus detection or using threat intelligence from your own forensic investigations or threat intel feeds. Scanning snapshots before recovery eliminates reinfection.

Accelerated Ransomware Recovery also solves the problem of data loss due to point-in-time recovery. Now you can automatically identify the most recent clean version of every file within a specified timeframe and consolidate those versions into a single "Curated Snapshot." Eliminating the manual search and recovery process drastically reduces the time to recover and prevents data loss.

druva


1. **Quarantine** infected resources and snapshots from the impacted dates.
Clean snapshots
Quarantined snapshots
2. **Restore** clean snapshots for business continuity.
3. Inspect and **delete** the quarantined snapshots.

Robust architecture and automated tools accelerate recovery and reduce data loss.

For IT and infosec managers and admins responsible for business continuity and resiliency, Druva's cloud-based ransomware protection and Accelerated Ransomware Recovery module prevent data loss, reduce costs, and accelerate ransomware attack response and recovery.

For more information

druva.com/use-cases/ransomware

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.

[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