perforce Delphix

Continuous Ransomware Protection

Continuously detect, protect, comply, and recover data

Challenge

Ransomware has become a national security concern and a major threat to businesses, with multiple cases of 10-day downtimes for mission critical applications. Cyber attackers are exploiting legacy security models of backup solutions and ingress often goes undetected for over 100 days to outlast data retention policies. In addition, traditional data restoration can take days and may need to be repeated multiple times, especially when victims are unable to determine the last clean state.

Modern ransomware attacks also include new variants beyond encryption, including lockerware (locking out victims from access) and extortionware or doxware, where data is exfiltrated and the threat of exposure is used to secure ransom payment. As cyber attackers continue to evolve, it's imperative that enterprises advance their ransomware preparedness.

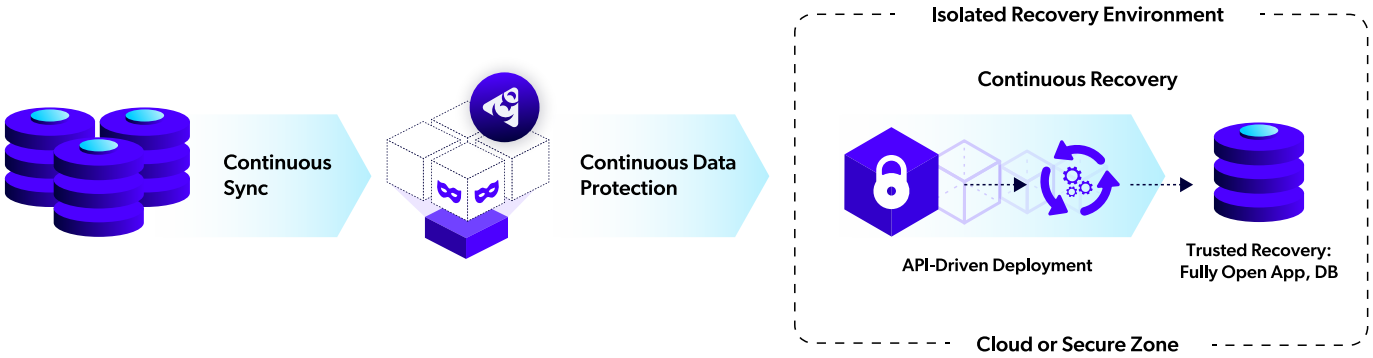
Solution

Delphix applies the power of DevOps to provide continuous ransomware protection. In a ransomware attack, companies need to rebuild applications and data quickly to a clean state from a historical point-in-time. With Delphix, teams can protect and recover enterprise applications using a more comprehensive solution compared to traditional once-a-day backups.

With the power and speed of DevOps, enterprises can build a resilient data backbone for enterprise applications that can quickly detect and recover from ransomware attacks using a robust set of APIs. With Delphix, teams no longer need bespoke or manual processes during stressful ransomware incidents and can consistently and reliably ensure the fast recovery of critical business information.

Key Benefits

- Immutably protect and recover data to any time down to the second or transaction boundary
- APIs for DevOps teams to automate the recovery of data alongside applications in isolated multi-cloud environments
- Early detection with automatic tests for block, file, and database encryption
- Automatically mask data to prevent extortionware
- Zero Trust architecture with layered security using industry best practices for encryption, authentication & authorization, access control, and auditing



Benefits

Continuous Data Protection

With Delphix, data is continuously synchronized in near real-time allowing teams to recover data from any point-in-time to the second[1] or database transaction. Once data is written into the Delphix DevOps Data Platform, all data changes are stored immutably in a Continuous Vault for the desired retention period and allows for many isolated virtual databases to be deployed from stored points in time.

Delphix's Continuous Vault prevents retention policy modifications or deletion of snapshots by attackers during breaches and can be isolated in different cloud regions or availability zones. In addition, Delphix can be deployed with object storage for elastic scalability that reduces costs for inactive data footprints.

Continuous Recovery

With Delphix, teams can ensure that they are prepared for ransomware attacks with tabletop testing and easily implemented regular drills to ensure recovery readiness. Using a rich suite of APIs, teams can automate the continuous synchronization of data into Delphix and build automatic inspection and re-deployment of data into isolated recovery environments that are immediately available as a hot spare during incidents. Alternatively, teams can instantly provision data from any point-in-time on-demand into multiple isolated recovery environments to manually inspect, test, and find the last clean state from the timeline within the immutable data time machine. In addition, the platform leverages zero trust architecture to protect access, stored data, and retention policies from tampering.

Continuous Detection

Delphix's ransomware protection solution empowers teams to detect attacks across a number of different vectors such as storage blocks, stored files, key changes, and data changes. Teams can integrate complex testing procedures as data is ingested into the immutable Continuous Vault to prevent any unscheduled data and metadata changes or identify tampering of credentials and encryption. With a rich suite of APIs and integration with FluentD, teams can integrate data events and metrics to 3rd party monitoring solutions as well as security information and event management (SIEM) solutions for better systems observability and improved response.

Continuous Compliance

Business continuity and compliance teams can now get ahead of data exfiltration attacks by continuously masking data in lower non-production environments to mitigate risk. Developer, Quality Assurance, Test, and Analytics environments often contain sensitive data and are much less protected than production environments. These environments are vulnerable to data theft and can contribute up to 70% of the risk surface. Delphix helps to profile and automatically mask sensitive data and personally identifiable information before it's delivered to development and analytics environments on demand. Teams benefit from the masking scale-out performance architecture that's able to continuously mask data and data changes.

1. Stats may change depending on specific database technology