DELPHIX

SOLUTION BRIEF

Continuous Ransomware Protection

Solving the Ransomware Challenge with DevOps

000332

Close Critical Gaps in Ransomware Protection

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 restores can take days and may need to be repeated multiple times, especially when victims are unable to determine the last clean state.

Ransomware attacks also include new variants beyond encryption, including lockerware (locking out victims from access) and extortionware, where data is exfiltrated and the threat of exposure is used to secure ransom payment.

It's imperative that enterprises advance their ransomware preparedness. Can you afford the 10 days of downtime other companies have faced?

Safeguard Your Most Critical Business Systems with the Speed and Power of DevOps

Delphix enables a DevOps approach for protecting enterprise applications. Applications laden with business critical data represent high-value targets for ransomware attacks, and high transaction change rates demand a specialized, more comprehensive solution than traditional once-a-day backups.

In a ransomware attack, companies need to repeatedly rebuild applications and data quickly to determine a clean state in time. With a DevOps approach, we enable you to rebuild your app from any time in the past, and integrate with CI/CD tools to automate the full recovery of applications, including underlying databases.

Delphix provides a foundational cyber and ransomware solution built on four pillars:

- Continuous data protection: Immutably protect and recover data to any time, down to the second or transaction boundary, storing data in a secure data vault
- Continuous recovery: APIs and automation to instantly recover applications to an isolated recovery environment
- Continuous detection: Automatically test data for block, file, or database encryption
- Continuous compliance: Automatically mask data to prevent extortionware

Continuous Data Protection: Minimize Loss, Maximize Confidence with Immutable Data And Isolated Environments

Delphix non-disruptively and continuously syncs data from source apps and databases in near real-time—down to the second or transaction. Delphix provides an immutable data time machine with a write-once, read-many (WORM) architecture. All change data is written to new data blocks (even data encrypted by ransomware), leaving the good data record completely unchanged and quickly accessible.

In addition, Delphix engines can be configured as data vaults, where retention policies cannot be manipulated and snapshots cannot be deleted, even by administrators. Snapshot and retention policy locks eliminate the risk of having insiders purposely delete protected data in concert with a ransomware attack.

Continuous Recovery: Instant Application, Database Recovery with Automated DevOps Builds

Once the data is in Delphix, the platform can quickly provision data to multiple environments with full automation for database parameterization and configuration. Delphix delivers open, online databases in just minutes. DevOps APIs allow teams to integrate with CI/CD tools to program databases into automated application builds.

Delphix is built on a scale-out architecture with data engines deployable on prem, across network security zones, across data centers, or across the multi-cloud. In addition, Delphix can efficiently replicate data from engine to engine, including to the cloud. With flexible, multi-cloud replication, Delphix can isolate data and provide a Zero Trust security model with support for OAuth and password vaults—enabling air-gapped isolated recovery environments (IREs) to prevent data loss and tampering. Leveraging IREs, teams can automate tabletop testing of recovery processes, rebuilding applications to different points in time to ensure readiness.

If an attack occurs, Delphix can quickly trigger an automated build of the environment state immediately prior to the ransomware event in just minutes.

In contrast, you can lose data from an entire day trying to recover from yesterday's backup, and recovery from full and incremental backups can take another day—a two day loss and recovery window.

Continuous Detection: Track, Test, Validate, Notify to Protect Against Multiple Attack Vectors

“Anomaly detection” from storage or backup solutions, which treat data as a closed box, leave enormous blind spots. To ensure data trust, Delphix provides detection across multiple attack vectors.

Delphix automatically tests for block, file, or database encryption on a continuous basis to combat extended dwell times and prevent “garbage in, garbage out” scenarios where teams feed recovery environments with bad data. Delphix also detects tampering or loss of encryption keys to protect against lockerware, where victims can be locked out from application or database access.

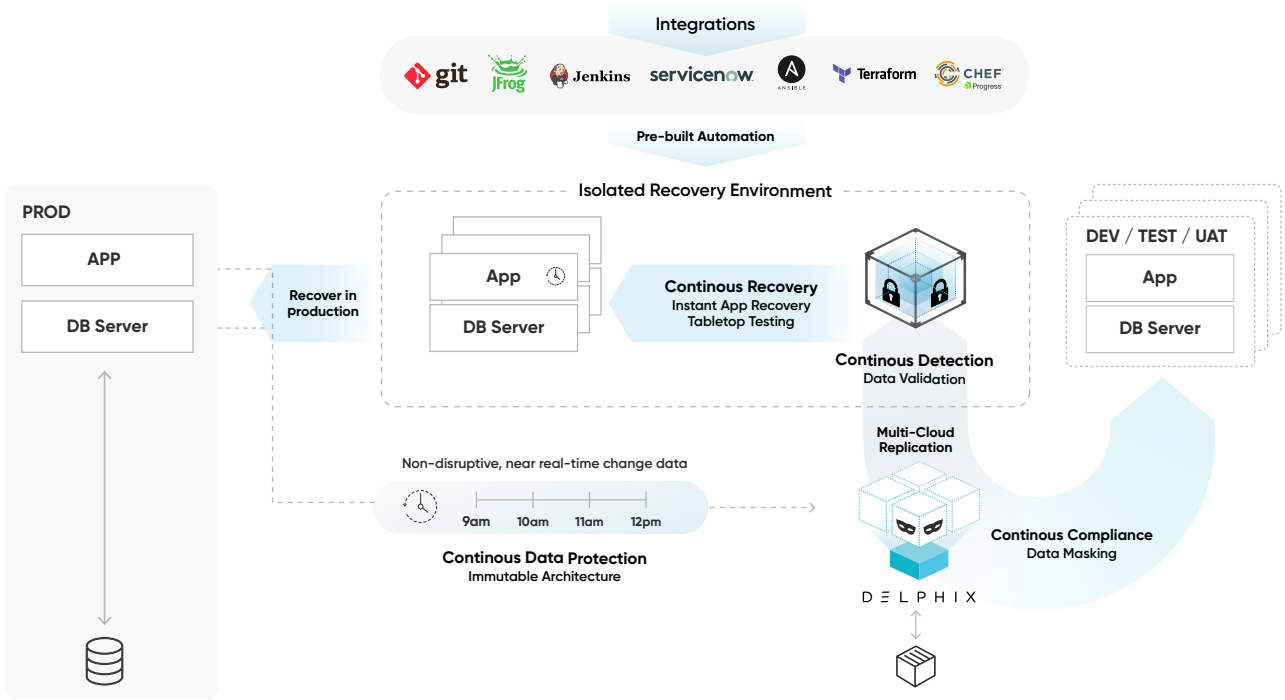
Finally, Delphix APIs can integrate with monitoring and automation tools, such as Splunk and ServiceNow, for real-time alerts and automated remediation.

Continuous Compliance: Safeguard Sensitive Data to Mitigate Risk of Theft

Over 70% of attacks combine data theft with encryption in order to secure ransoms from target victims. Delphix defends against theft in non-production data environments (80-90% of total data) to mitigate extortionware risk. Delphix provides integrated data profiling, masking, and automated delivery of compliant data for development, testing, and CI/CD workflows.

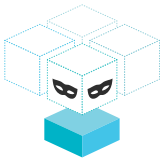
A scale-out performance architecture enables efficient masking for large data stores in private and public clouds, including SaaS. Continuous masking of change data provides an alternative to batch-style jobs to provide secure data in near real-time.

How It Works: **Continuous Ransomware Protection**



The DevOps Data Platform Advantage

Delphix provides the most sophisticated and complete solution for enterprise application and database resiliency. Compared to alternative backup solutions, Delphix provides the following comparative benefits:

Backup Solutions	DELPHIX 
General purpose backup for files, VMs, etc.	Advanced solution for **enterprise applications, database**
Backup can be deleted, overwritten with encrypted data when credentials compromised — full data loss	Immutable data vault: WORM, zero trust architecture, locked retention policies, replication to **isolated recovery environment**
Major data gaps: once daily backups	**Continuous data protection:** recover down to the second with highest efficiency for long retention coverage*
Manual, incomplete restore process requiring multiple admins — restore time in days	**Instant application recovery at scale** automated via DevOps APIs + zero trust security model + performance caching
Closed-box approach does not check multiple levels for encryption or test and validate data being backed up — long dwell times, data loss	**Continuous detection** for blocks, files, keys, data — eliminate dwell time and 'garbage in — garbage out', early detection, response
No solution for data theft, privacy compliance	**Mask** all non-production data (80-90% of total data)
Pre-digital solution when slow restores acceptable	**DevOps data platform for instant, automated, trusted recovery**

* Continuous data protection is for Oracle, Microsoft SQL Server, and SAP ASE. Daily or more frequent snapshots are provided for all other data sources.

Continuous Ransomware Protection

DELPHIX

Delphix is the industry leading data company for DevOps.

Data is critical for testing application releases, modernization, cloud adoption, and AI/ML programs. We provide an automated DevOps data platform for all enterprise applications. Delphix masks data for privacy compliance, secures data from ransomware, and delivers efficient, virtualized data for CI/CD.

Our platform includes essential DevOps APIs for data provisioning, refresh, rewind, integration, and version control. Leading companies, including UKG, Choice Hotels, J.B. Hunt, and Fannie Mae, use Delphix to accelerate digital transformation. For more information, visit www.delphix.com or follow us on LinkedIn, Twitter, and Facebook.

000332