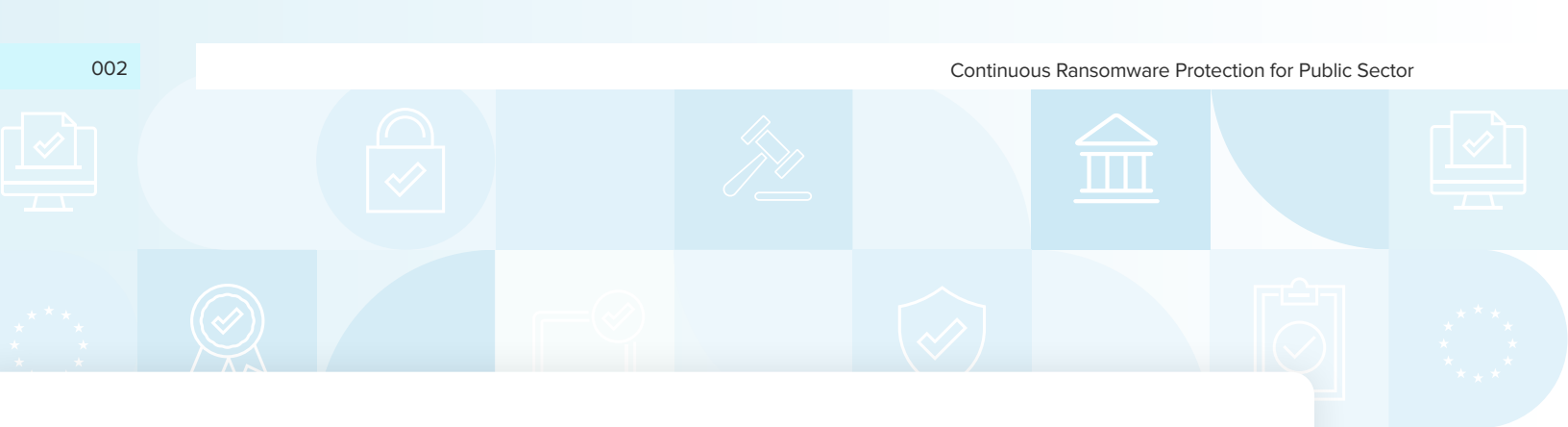




# Continuous Ransomware Protection for Public Sector



Ransomware has become a national security concern and major threat to agency enterprise applications, with multiple cases of 10-day downtime events. Attackers are exploiting legacy security models of backup solutions and ingress often goes undetected for over 100 days. In addition, traditional restores can take days and may be repeated when victims are unable to determine the last clean state.

Attacks 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.

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, rewinding data to any point in time.
- » **Continuous Detection:** Automatically test data for block, file, or database encryption.
- » **Continuous Compliance:** Automatically mask data to prevent extortionware.

# Solving the Ransomware Challenge with DevOps

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.

## Continuous Data Protection

Agency data in enterprise applications and databases changes rapidly. Delphix non-disruptively and continuously syncs data from source apps and databases in near real-time into an immutable data time machine with a “write-once, read-many” architecture. Teams can configure Delphix engines as secure data vaults, preventing retention policy modifications or deletion of snapshots.

## Continuous Recovery

Delphix recovers data from any time down to the second or transaction, with automation to provision open databases in minutes. DevOps APIs allow agencies to integrate with CI/CD tools to program data into automated application builds. Recovery can occur from air-gapped, isolated recovery environments enabled through multi-cloud data replication. Leveraging those environments, teams can automate tabletop testing of ransomware recovery. If an attack occurs, Delphix quickly triggers an automated build of the environment state immediately prior to the ransomware event.

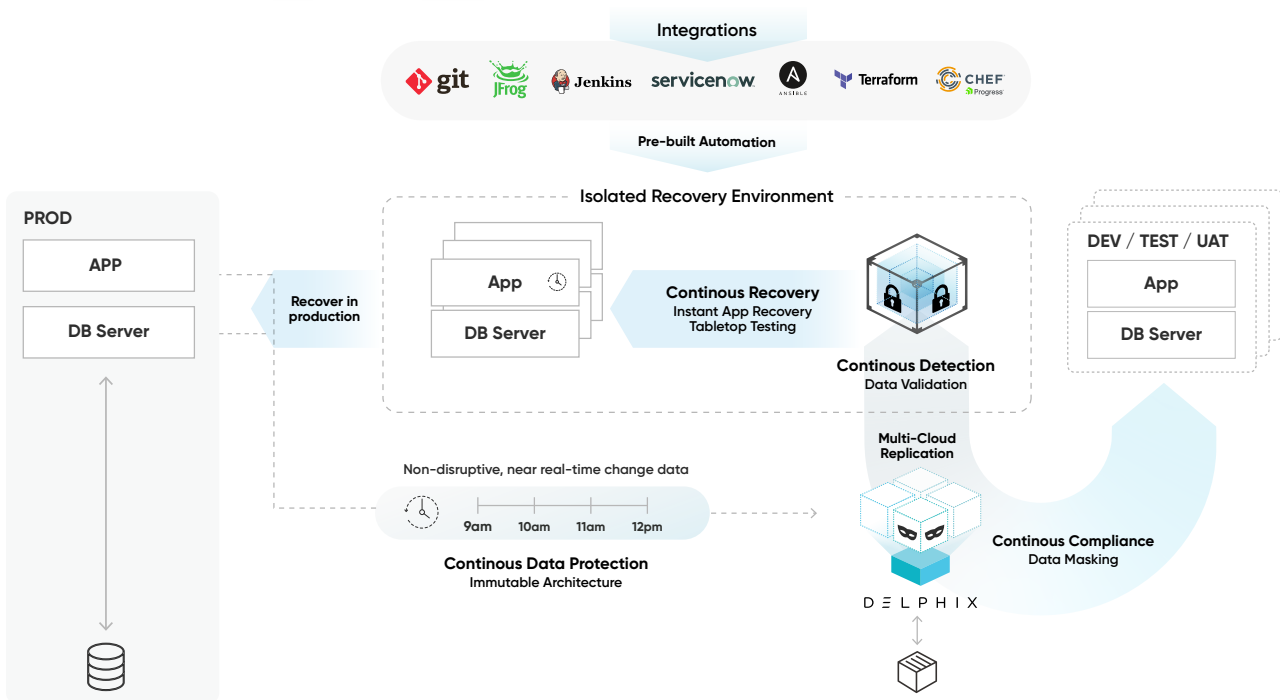
## Continuous Detection

To prevent long dwell times and ensure data trust, Delphix provides detection across multiple levels of attack vectors. Delphix automatically tests for block, file, or database encryption and detects tampering or loss of encryption keys. APIs enable easy integration with SEIM tools such as ServiceNow, to streamline alert and response workflows

## Continuous Compliance

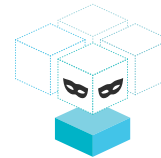
Delphix defends against data theft in development and analytics environments. Delphix profiles and automatically masks sensitive data and personally identifiable information, then automates delivery of secure data to non-production environments. Masked non-production data (80-90% of data) mitigates risk of data theft via extortionware.

## How It Works: Continuous Ransomware Protection



# The Delphix Advantage

Delphix provides the most complete ransomware solution for public sector enterprise applications. Compared to backup solutions, Delphix provides the following comparative benefits:



## Backup Solutions

DELPHIX

General purpose backup for files, VMs, etc.	Advanced solution for <b>enterprise applications, database</b>
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 <b>isolated recovery environment</b>
Major data gaps: once daily backups	<b>Continuous data protection:</b> recover down to the second with highest efficiency for long retention coverage*
Manual, incomplete restore process requiring multiple admins — restore time in days	<b>Instant application recovery at scale</b> 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	<b>Continuous detection</b> for blocks, files, keys, data — eliminate dwell time and ‘garbage in — garbage out’, early detection, response
No solution for data theft, privacy compliance	<b>Mask</b> all non-production data (80-90% of total data)
<b>Pre-digital solution when slow restores acceptable</b>	<b>DevOps data platform for instant, automated, trusted recovery</b>

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

## 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](http://www.delphix.com) or follow us on [LinkedIn](#), [Twitter](#), and [Facebook](#). ©2021 Delphix