Secure Data Across Application Landscapes:
On Premise, Offsite & In the Cloud

REINVENTING DATA MASKING

WHITE PAPER

TABLE OF CONTENTS

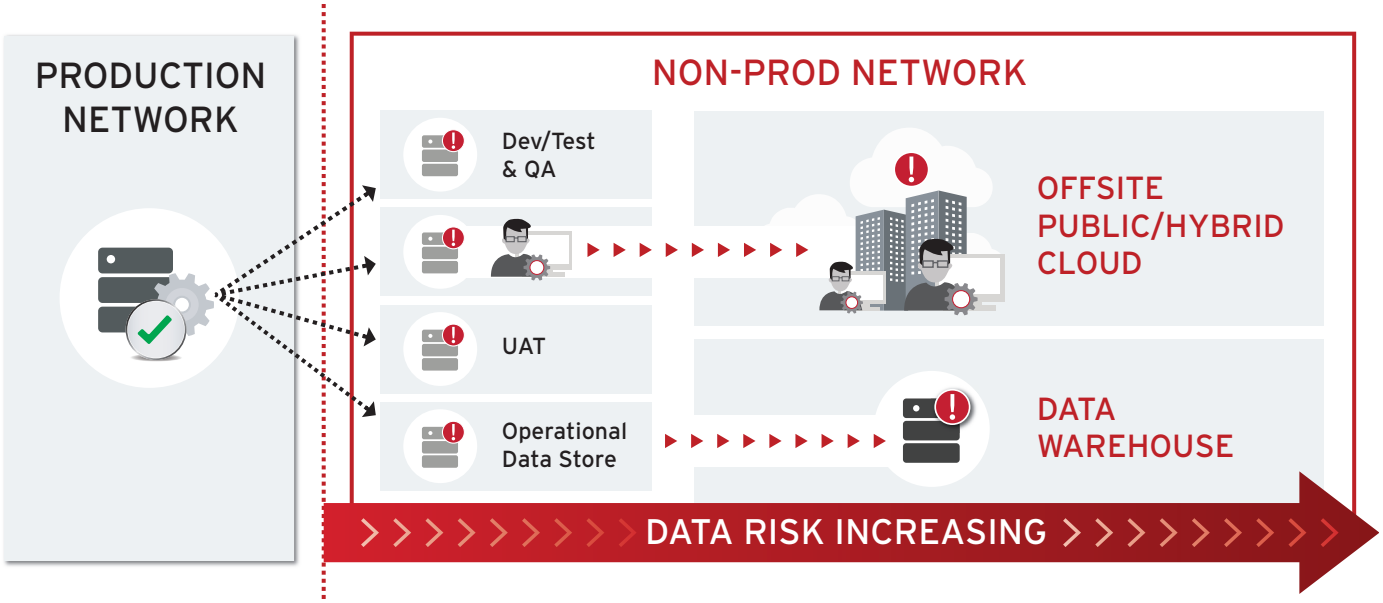
DATA PROTECTION CHALLENGES ACROSS APPLICATION LIFECYCLES

Digitization and data breaches have led to increased privacy regulation across regions and industries. Privacy mandates like PCI, HIPAA, GLBA, FERPA, and ITAR have gone through multiple revisions that have increased noncompliance penalties and tightened enforcement. Across sectors, organizations are struggling to meet the growing pressure to protect sensitive internal or customer information in an efficient and cost-effective manner.

Production instances of applications are generally where sensitive data is captured and introduced. However, the data protection challenge extends far beyond production systems. For every unit of sensitive data that resides in a production environment, numerous copies are created and propagated both upstream, for software development and testing, and downstream, for analysis and reporting. Collectively, these copies account for 80% or more of all sensitive data and risk exposure in organizations.

LARGE SURFACE AREA OF RISK ACROSS APPLICATION LIFECYCLE ENVIRONMENTS

AS DATA MOVES INTO NON-PRODUCTION OR LESS SECURE NETWORKS—ESPECIALLY OFF SITE TO THIRD PARTIES OR INTO PUBLIC AND HYBRID CLOUDS—THE DATA CHANGES CONSTANTLY AND THE SURFACE AREA OF RISK INCREASES.



Data masking solutions are designed to obfuscate and protect sensitive data across application lifecycle environments. However, application data is continuously changing and growing. This introduces the need for constant data movement and updates across environments. For example, reporting copies need the latest transactions from production for timely operational analysis. Similarly, development copies need to be frequently updated to ensure thorough testing against the latest state of production. Alternately, data may have to be pushed from a QA environment back to a development instance for analysis of a software bug.

Traditional data masking solutions primarily focus on the rules and logic of data obfuscation. Broad usage of such masking tools has been limited by the high cost of repeating data masking steps each time data is distributed to a development, test, reporting or other copy. As a result, organizations often entirely avoid the overhead of repeated masking and instead use artificially generated data in development and testing, which in turn erodes application quality. Similarly, the complexity of distributing masked data creates pushback from IT security and compliance teams around adoption of new or alternate IT models like outsourcing, offshoring, and public or hybrid cloud systems.

DELPHIX SERVICE-BASED MASKING OVERVIEW

Delphix Service-Based Masking is the only solution that tackles both generation and distribution of masked data. By combining patented data masking techniques with market-leading virtual data delivery capabilities, Delphix eliminates the limitations of traditional masking solutions. With Delphix, application teams get full, fresh, and secure data sets in minutes. Delphix virtual copies can be refreshed in minutes, bookmarked and rolled back to previous points in time, and branched or mapped to specific code builds, with end-user self-service and 90% less infrastructure. As a result, organizations can meet the requirements of privacy regulations faster and at a lower cost.

Delphix Service-Based Masking enables sensitive data protection across all application lifecycle environments. For nonproduction environments, Delphix performs persistent masking on specified databases and files, ensuring full protection for sensitive data. Additionally, Delphix replication enables rapid, secure, bandwidth efficient delivery of masked data to third parties and cloud providers. This eliminates security and compliance related objections to offshoring, outsourcing, and cloud adoption. Delphix makes it possible to entirely offload unauthorized users from production to cost effective, synchronized, and masked virtual copies.

DELPHIX DATA AS A SERVICE (DAAS)

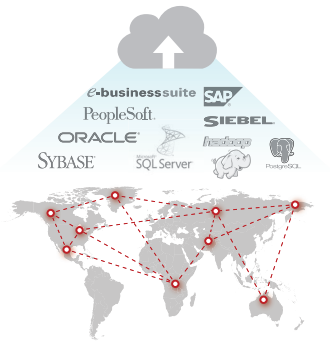
The power of Delphix Service-Based Masking is rooted in virtual data delivery. Instead of repeatedly making and moving physical data copies, Delphix provides a virtualized instance of databases, applications, and files by abstracting data from hardware and storage. Through intelligent data block mapping and sharing, Delphix eliminates widespread data redundancy and creates a compressed master copy of the production environment.

Delphix can then provision virtual environments for development, testing, QA, integration, reporting, sandboxes, backup, and data recovery. These virtual environments function just like full physical copies, but consume a fraction of the space and can be created in a fraction of the time. Further, Delphix maintains synchronization with production by collecting changes and tracking all versions for as long as required. Delphix non-disruptive synchronization eliminates 95% of source and network load caused by full data extraction and movement, and each virtual instance can be quickly and automatically refreshed to provide full data from any point in time.

By consolidating and sharing data blocks across copies, Delphix can eliminate over 90% of the surface area of data exposure to breaches. Additionally, Delphix provides strong, centralized logging and reporting on data environment access for audits.

The capabilities of Delphix DaaS are supported across a large number of data sources and delivered as a software virtual appliance referred to as the Delphix Engine. The virtual appliance form factor of the Delphix Engine maximizes deployment flexibility, scale, availability and cloud readiness.

VIRTUALIZE

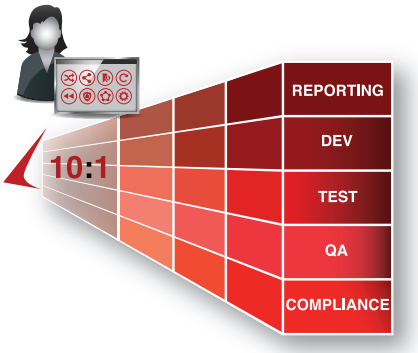


- Efficient, near real-time
- 10x less bandwidth required
- Any app, server, storage

GOVERN

- Secure copies on-demand
- Manage release versions
- Store 30 days in space of 1

DEPLOY

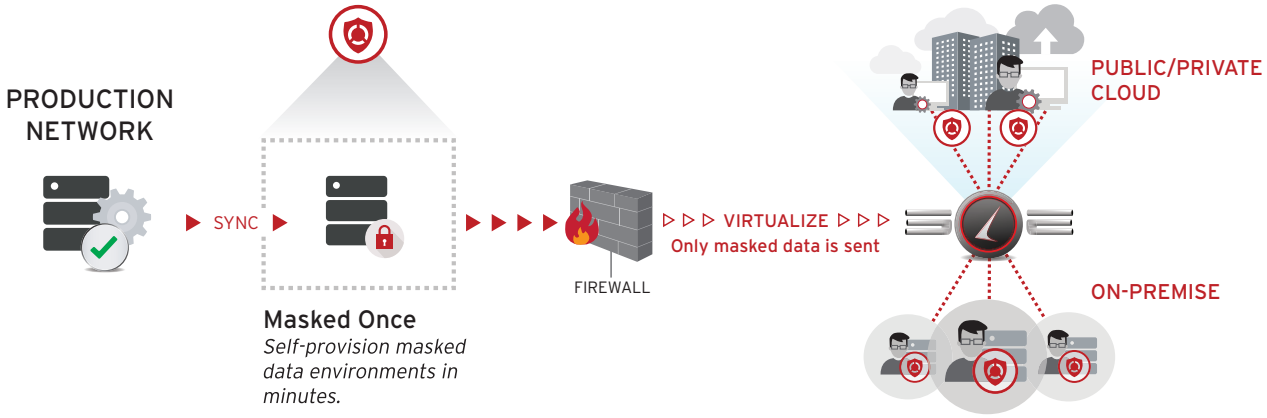


- Run 10 copies in space of 1
- 10x time, storage savings
- On-premise, offsite, cloud

MASKING SCENARIOS WITH DELPHIX

1. PERSISTENT MASKING

The risk profile of some critical applications processing sensitive data may warrant masking every derived copy. Persistent Masking with Delphix is an effective approach for this scenario. Data is first masked in a staging environment that is built from the production source. The Delphix Engine links to and synchronizes with this masked staging environment. As a result, all data managed by Delphix for this application is always masked. From the masked data timeline managed by Delphix, secure virtual copies can be created and distributed on-demand and via self service by requesting users.



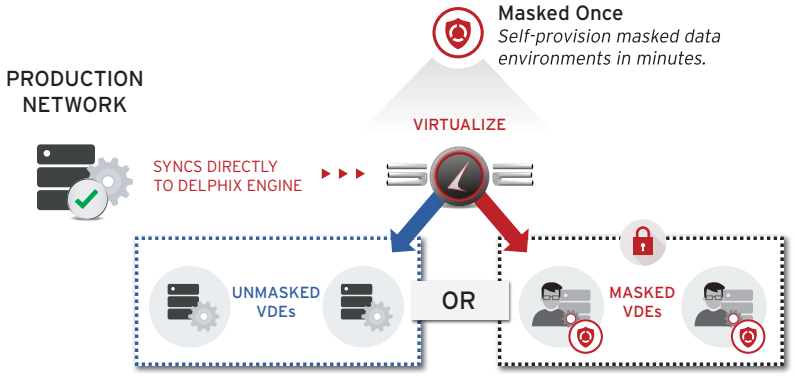
This method of masking in production ensures that no sensitive data leaves the production environment. Because the Delphix Engine is linked to the masked staging environment, all virtual copies provisioned for non-production use are automatically secure. This is ideal for scenarios in which regulatory compliance requires that only secure data be allowed to leave the production environment. Delphix also enables rapid provisioning of masked data to cloud environments. As with on-premise masking, Delphix masking in the cloud supports several architectures, allowing organizations to meet a wide range of security, agility, and compliance needs.

- **DIRECT SYNC:** Delphix is installed in the cloud and connects directly to on-premise production systems over a secure, encrypted channel. It then provisions masked virtual copies across the cloud. This method of masking enables cloud delivery of both masked and unmasked data.
- **DISTRIBUTED SYNC:** In this scenario, Delphix is installed on-premise as well as in the cloud. The Delphix Engine deployed on premise synchronizes with the production source and then replicates to the Delphix Engine deployed in the cloud. This provides greater flexibility and availability. For example, the local Delphix Engine can produce both masked and unmasked copies but only replicate secure copies to the Engine in the cloud.

2. SELECTIVE MASKING

Many applications that capture and process sensitive data require both clear and masked copies. For example, regulations might dictate that developers cannot have access to sensitive data of customers. However, internal business analysts may be authorized to access all data in the clear for accurate financial reporting and business performance analysis. Selective masking is the appropriate path in this scenario.

Selective masking involves execution of masking against a virtual copy created by Delphix. The Delphix Engine links directly to the production source rather than through an intermediary masked staging environment. From its unmasked master copy, Delphix then facilitates the quick and easy creation, refresh, bookmarking, and sharing of both masked and unmasked virtual data environments (VDEs) for non-production use. Virtual copies are initially created as unmasked copies and then the masking process is applied. The data is read, masked to administrative specification, and loaded back into the Delphix engine, thereby eliminating all traces of the clear, sensitive data. Only after the masking is complete is the non-production team granted access to the masked virtual data. Meanwhile the business analysts can directly create and refresh copies in the clear.



- Delphix Engine links directly to production
- VDEs provisioned from Delphix Engine can then be masked or left clear
- Different VDEs are deployed per use case/user role

THIS METHOD OF MASKING FOR NON-PRODUCTION ENVIRONMENTS HAS A NUMBER OF ADVANTAGES:

1. **ENABLES THE PROVISIONING OF BOTH MASKED AND/OR CLEAR COPIES**
   Giving authorized teams access to clear, unmasked data for uses such as production support or business intelligence while unauthorized users are limited to masked copies.

2. **ALLOWS DISTINCT MASKING POLICIES FOR EACH VIRTUAL COPY**
   Supporting varying sensitive data restrictions by developer or team.

3. **FASTER EXECUTION AND DATA REFRESH WHEN DELPHIX LINKS DIRECTLY TO THE PRODUCTION SOURCE**
   The synchronization process only involves pulling incremental changes from the source. This also reduces overall load on the production system.

4. **VIRTUAL COPIES CAN BE CREATED FROM ANY POINT–AT ANY TIME**
   Delphix is continually synthesizing the incremental changes–down to the second or transaction boundary.

SUMMARY

Widespread use of traditional data masking solutions has been limited by the high cost of repeating data masking steps each time data is distributed to development, test, reporting or other copies. Delphix is the first solution to eliminate the distribution challenges of masked data. With Delphix Service-Based Data Masking, sensitive data only needs to be masked once, after which copies and updates can be delivered to any location in minutes. This eliminates compliance-driven pushback to cloud adoption and offshoring. Additionally, application teams get full, fresh, and secure data sets in minutes. Lastly, Delphix reduces the surface area of data exposed to breaches through consolidation and centralized auditing of sensitive data access.

Industry regulations often require that organizations mask sensitive data such as personally identifiable information or protected health information. Organizations themselves may also seek to protect company and employee information. Some examples of regulatory standards that require the masking of sensitive information include:

HIPAA—the Health Insurance Portability and Accountability Act regulates the manner in which actors within the healthcare and pharmaceutical industries transmit sensitive Patient Health Information. Sections 164.514(a), (b), and (c) of the HIPAA Privacy Rule set the standard for the de-identification of protected health information and contain the implementation specifications that require individually identifiable health information such as names, locations, dates, and medical records be located and masked.

PCI DSS—the Payment Card Industry Data Security Standard regulates all organizations that handle cardholder information for major credit, debit, and ATM cards. Requirement 3 of PCI DSS details technical guidelines for protecting stored cardholder data, requiring that primary account numbers and associated identifiable information be masked and rendered unidentifiable at all points in storage.

FACTA—the Fair and Accurate Credit Transactions Act allows consumers to request and obtain a free annual credit report from each of the nation's consumer credit reporting agencies and seeks to prevent identity theft. Under FACTA, full credit account numbers and expiration dates must be truncated or masked when reported. Further, credit reporting agencies may not disclose the personally identifiable information of any medical creditor unless it is masked to conceal the individual's condition and provider.

Reinventing Data Masking
May 2015

You can find the most up-to-date technical documentation at:
http://www.delphix.com/support

The Delphix Website also provides the latest product updates.
If you have comments about this documentation, submit your feedback to:
help@delphix.com

Delphix Corp.
275 Middlefield Road, Suite 210
Menlo Park, CA 94025
www.delphix.com