DELPHIX

Five Steps Towards Achieving Secure Data Flow

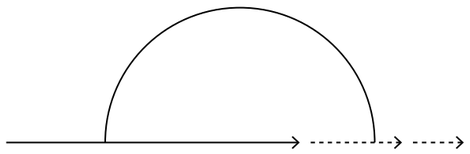
Resolving the Tension Between Data Security and Data-Driven Innovation

Let Data Flow.

"The big aren't eating the small. The fast are eating the slow."

The Innovation Imperative

This now familiar refrain does well to capture today's attitude about data-driven innovation: Transformation must happen now.



Disruptive business models enabled by the confluence of DevOps, Cloud, and AI/ML—and fueled by enterprise data—on one hand embolden nimble startups to move faster, while on the other force established leaders to redouble their efforts to effect data-driven change.

Managing Data In the Age of Breach

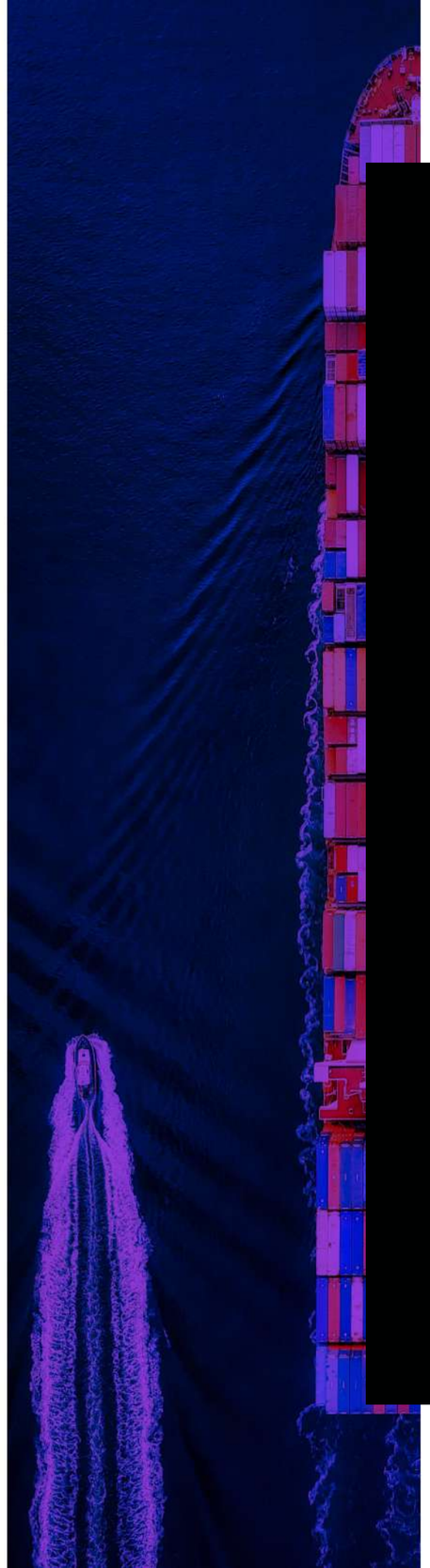
But at what cost? The narrative surrounding enterprise data has taken a beating as a slew of breaches and cases of misuse have made headlines. From Equifax to Uber, companies that have prioritized speed and innovation over security and thoughtfulness have been exposed. Their peers and the public have taken note.

Simultaneously, the emergence of stringent data privacy regulations such as GDPR puts additional pressure on businesses across

Progress Versus Protection?

Dueling priorities of fast innovation vs. security meet head on in the modern enterprise.

Projects that move the needle—from cloud adoption to custom application development to building machine learning algorithms—demand a fast flow of data without setting off alarm bells for security teams. At the same time, requirements for security and compliance may be perceived as standing in the way of transformation. A recent survey by the Economist found that:



54%

of corporate management said that measures to prevent cyber attacks absorb too much management time.

45%

percent said attention to these processes slow competitive response.

Retail

Consumer data such as payment information feeds retail analytics systems but must be secured to protect against breach and comply with regulations such as PCI-DSS.

Banking

Test datasets used to build online and mobile banking applications must be free of personal information before being exposed to development teams.

Education

Schools must protect faculty and student information including academic performance, admissions records, and financial information across back-office apps and student-facing portals.

Life Sciences

Clinical study participant data needs to be "de-identified" in a way that protects personal privacy, while still preserving the value of the data for R&D.

Healthcare Providers

Electronic Health Records (EHR) and Electronic Medical Records (EMR) systems revolutionize patient care but challenge providers to protect patient health information for compliance with regulations such as HIPAA.

Manufacturing

The rise of IoT creates opportunities to develop a new generation of connected devices, but also heightens privacy risks with more customers sharing more information traceable to a person or a household.

Secure Data Flow

Balancing Rapid Innovation with Privacy and Security

	INNOVATION LAGGARDS	INNOVATION LEADERS
SECURITY LEADERS	Data is locked down, unavailable to fuel transformation	Secure Data Flow: Fast, easy access to the right data in a safe manner
SECURITY LAGGARDS	Data remains rigid, siloed, and unprotected	Data drives transformation but exposes organization to unnecessary risk

The overwhelming necessity to drive both innovation and security means that companies can't abandon one priority in favor of the other. Rather, they need to treat innovation vs. security as a false duality, and seek out ways to become secure disruptors that advance both causes.

And when it comes to the enterprise data that fuels innovation (while simultaneously serving as a source of vulnerability), businesses need to adopt processes and technologies that allow data to flow freely across the enterprise. After all, data isn't valuable if no one has access to it.

Current security solutions trap data in silos and deter adoption by adding complexity. What modern enterprises need, instead, is a solution that aligns with goals around innovation—one that puts security at the heart of innovation, speeding up important initiatives instead of slowing them down. More specifically, enterprises need an approach that helps them realize secure data flow through the following key steps:

1 **Discover Your Data:**
Establish an enterprise-wide view of your data environments.

2 **Mask Your Data:**
Protect sensitive data while ensuring it's usable by data consumers.

3 **Deliver Your Data:**
Provide a means to quickly distribute data to those who need it.

4 **Govern Your Data:**
Control who has access to what data, when, and where.

5 **Extend and Embed:**
Integrate with the technologies and processes your business depends on.

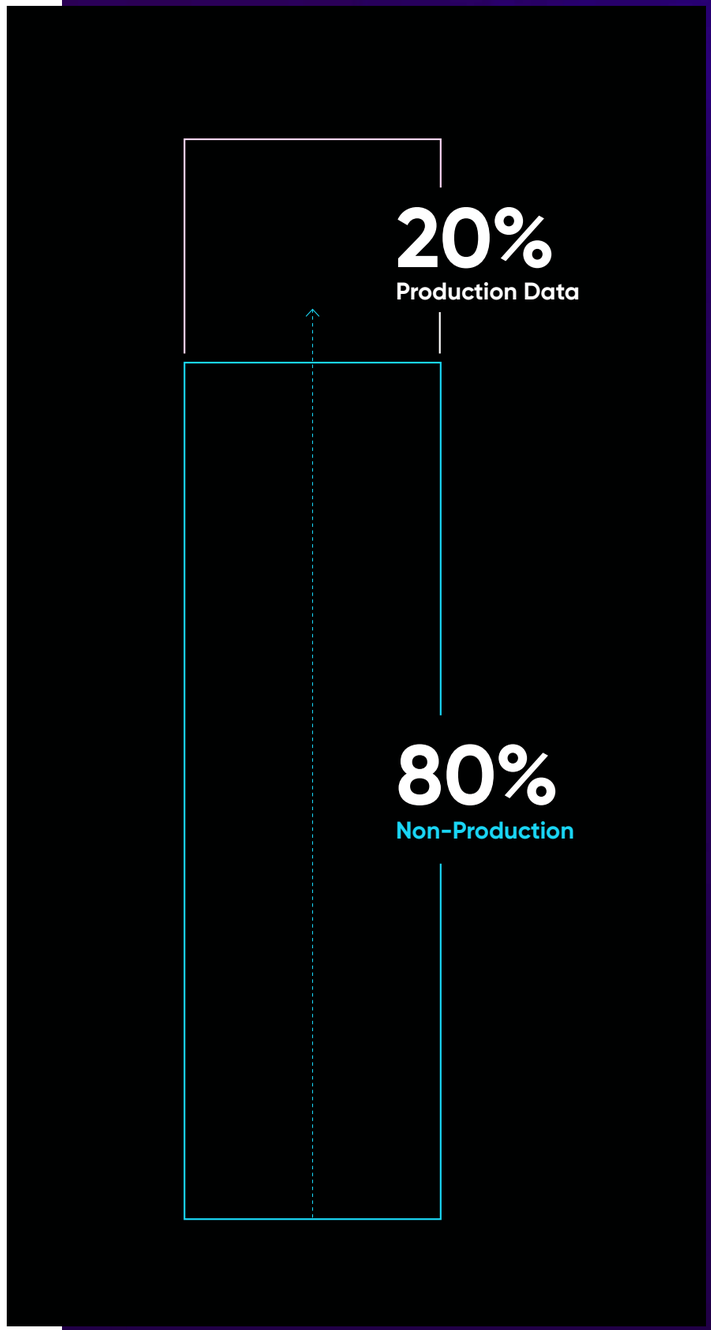
DELPHIX

Discover Your Data

Establish an enterprise-wide view of risk

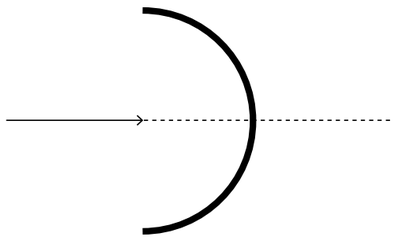
Enterprise data is estimated to grow 10x by 2025[1]. Fueling this data explosion is the sprawl that results as production data is copied for development, testing, production support, backup, or reporting. These so-called "non-production" data environments drive key projects for application development, cloud migration, or advanced analytics. But they also represent a huge hidden risk, containing the vast majority of an enterprise's sensitive data.

Enterprises that hope to protect sensitive data must discover it first. Security solutions must easily identify names, addresses, credit card numbers, and other confidential information, particularly across non-production landscapes. Doing so gives businesses an enterprise-wide view of risk that helps them deploy the right protective measures in a targeted manner.



Non-Production Data:

- Constantly growing
- Entails multiple types of repositories
- Often less protected by security and governance measures



Data Discovery Checklist:

- ☐ **Automated processes** eliminate manual checks and validation
- ☐ **Pre-built accelerators** speed sensitive data identification for specific apps (e.g. SAP or PeopleSoft) and regulations (e.g. GDPR or HIPAA)
- ☐ **Tailored discovery** via regular expressions pinpoints information deemed sensitive by business requirements or specific regulations
- ☐ **Broad support** to discover data across a wide range of data source types, including RDBMS, file, and Big Data sources

[1]Source: IDC

2

Mask Your Data

Protect sensitive data so it can be freely shared

Effective discovery paves the way to protecting information with a masking solution that transforms sensitive data values into fictitious, yet realistic equivalents. Data masking is the de facto standard for securing non-production data because it neutralizes insider and outside threats, while preserving the value of the data to users.

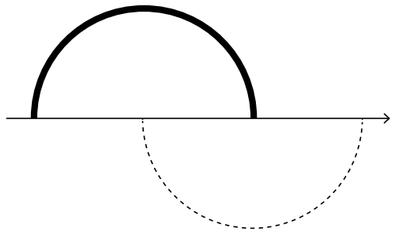
Once data has been irreversibly masked, it can be freely shared internally or externally without risk of loss, and in full compliance with key data privacy regulations.

Unmasked

Last Name	Phone
Lee	415-230-1283
Rogers	510-512-5123
Lee	317-512-4489
Jacobson	650-965-1117
Sanchez	310-634-8145

Masked

Last Name	Phone
Jones	905-263-7354
Frank	847-512-5472
Jones	415-612-8452
Williamson	312-623-3833
Jones	708-512-5647



Data Masking Checklist:

- ☐ **Irreversible** masking ensures data cannot be restored to its original, sensitive state
- ☐ **High-fidelity, masked data** that doesn't compromise development, testing, reporting, or other key use cases
- ☐ **Pre-defined masking algorithms** plus the ability to develop custom or net-new routines
- ☐ **Referential integrity** for masked data to preserve important data relationships

B|E|C|U

Delphix addresses the first crucial step in securing sensitive data for Boeing Employees' Credit Union, the 4th largest credit union in the US: Discovering where the risk lies by using a built-in data discovery tool. Next, Delphix provides masking frameworks that require no programming knowledge or administrative involvement to create custom algorithms.

Key Facts:

- BECU masked 662 tables, 3,507 columns, and 680 million rows of data in 15 hours
- They completed the implementation in 6 weeks, meeting compliance requirements ahead of schedule. BECU estimated that competitors' tools would have taken an estimated 18-24 weeks to deploy.

"Not only does Delphix allow us to reduce our risk footprint by masking sensitive data, but we can also give developers realistic, production-like environments, which ensures we're not introducing defects because of bad data."

—Kyle Welsh | Chief Information Security Officer, BECU

3

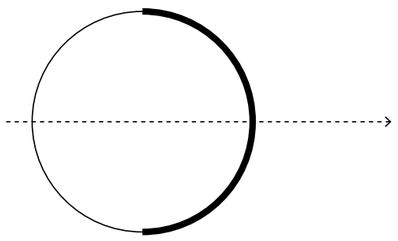
Deliver Your Data

Distribute data to those who need it

Data masking is only practical when it's coupled with an effective approach for distributing the data once it's been secured. Unfortunately, most organizations rely on a request-fulfill model for data delivery that involves IT service tickets, manual effort, and coordination across multiple teams.

A recent data management survey found that, on average, it takes 3.5 days and 3.8 individuals to fulfill a request for a new data environment in an enterprise setting. The same survey found that at 1 out of 5 organizations, data delivery takes over a week.[2]

However, a platform-based approach to data provisioning helps businesses streamline their delivery processes and achieve secure data flow. By integrating automated masking with modern data virtualization into a single platform, businesses can continuously deliver masked data copies to downstream environments in minutes instead of days or weeks.



Data Delivery Checklist:

- ☐ **Fast and automated** data delivery models eliminate slow, manual processes and reduce errors
- ☐ **API-driven** approaches enable easy integration into SDLC and analytics workflows
- ☐ **Broad support** for data sources within the on-premises, cloud, and hybrid environments that your organization depends on
- ☐ **Self-service controls** allow data consumers (developers, testers, analysts, etc.) to access and control data without administrative intervention

eharmony

eHarmony leveraged Delphix to implement a self-service data management solution, enabling development and QA teams to create and refresh environments as needed, without the involvement of DBAs. Refreshes can now be completed in an hour, delivering relevant and accurate data to development teams on demand.

Key Facts:

- 5000 Hours of projected labor savings over a three year period
- 60 Minutes to refresh multi-terabyte databases

Delphix delivers the environments we need for Dev, Test, and QA to enable our Agile and DevOps methods. We improved our data masking capabilities, minimizing risk. Delphix is a no-brainer."

—Navdeep Kumar | Senior Director, eHarmony

[2]Source: Techwell

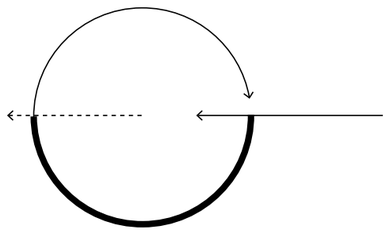
4

Govern Your Data

Control who has access to what data, when, and where

Two forces stand diametrically opposed to each other in the modern enterprise: The growing need for data consumers including developers, testers, analysts, and data scientists to easily access data, and the need for data managers such as DBAs, system admins, and information security professionals to ensure that data is carefully controlled.

A modern approach to data governance must serve the needs of both these constituencies. Locking down data indiscriminately isn't a effective governance model. At the same time, enterprises must limit privileged user access, maintain full control of data availability and retention, and ensure that data controls can be embedded into key workflows.



Data Governance Checklist:

- ☐ **A single point of control** for maintaining and deploying data governance policies
- ☐ **Permissions** to determine who has access to what data, where, when, and for how long
- ☐ **API-driven approach** to integrating controls into workflows for securing, managing, provisioning, and de-provisioning data
- ☐ **Reporting and audit** capabilities that track access, record security actions, and build a chain of custody for data

DENTEGRA

To protect cloud data from breach and to enable regulatory compliance, Dentegra needed to secure sensitive data before moving it to AWS. The Delphix platform collects data from Dentegra's production applications and applies masking to that data to protect any confidential information. It then replicates masked data to AWS where teams can instantly provision virtual, space-efficient data copies to dev/test environments running on AWS EC2 instances.

Key Facts:

- Delphix reduced the time it takes to move data to cloud environments from 8 weeks to hours.
- Delphix masks sensitive personally-identifiable information (PII) and patient health information (PHI) before replicating it to AWS environments.

"The combination of Delphix and AWS gives us the agility we need to succeed in today's application-driven economy. By easily and securely moving data to the cloud, we're able to release new features to the market faster, while also lowering cost and risk."

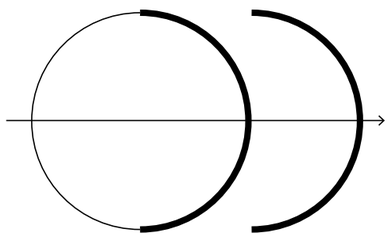
—Shan Swaminathan | VP of Application Delivery and DevOps, Dentegra

Extend and Embed

Integrate your solution with key technologies and processes

Achieving secure data flow is an imperative that touches your entire organization, from the CISO and CIO, to IT and applications leaders, down to individual developers and analysts. Given the breadth of stakeholders, technologies, and workflows that tap into enterprise data, your data security and management challenges can't be effectively addressed through a point solution—or even a set of point solutions.

Data security should be designed into the key processes that drive your business, rather than bolted on after the fact. A platform-based approach will allow you to easily integrate with the technologies your business depends on (e.g. for access control or data loss prevention) as well as your key processes (for the SDLC, reporting, audit, risk management) to ensure your solutions are adopted and effective.



Extensibility Checklist:

- ☐ **Platform-based approach** to enable easy integration with complementary solutions
- ☐ **Out-of-the-box support** for multiple, heterogeneous data sources with extension points to support future sources
- ☐ **Scalability** to apply data masking and data governance policies across the entire enterprise in a consistent fashion
- ☐ **Full API set** and cookbooks to embed data capabilities into business-critical workflows

DELPHIX

THE CLOROX COMPANY

"The biggest benefit of Delphix for us is time, getting things done faster, in hours, instead of days or weeks. Also, because we're now able to test in current environments with realistic, working datasets, we've seen a material improvement on quality, a reduction of risk, and a proven ability to apply new solutions to the business."

—Ralph Loura | Former CIO, Clorox

MOLINA HEALTHCARE

"In my four years as CIO here at Molina, the best ROI of any technology investment that I've made has been with Delphix."

—Rick Hopfer | CIO, Molina Healthcare

Let Data Flow.

About Delphix

Delphix's mission is to free companies from data friction and accelerate innovation. Fortune 100 companies use the Delphix Dynamic Data Platform to connect, virtualize, secure and manage data in the cloud and in on-premise environments.

The Delphix Dynamic Data platform serves as the foundation for DataOps across hundreds of the world's leading enterprises. By implementing data pods and increasing secure data flow to the business, leading companies across industries have unlocked significant outcomes trapped in their development and IT investments.

Flawless go live for hundreds of divided apps in separation into HPI and HPE

30% increase in year-over-year sales by enabling superior mobile user experience

Recovery of Video on Demand service for 24M users in minutes initiatives.

Tripled revenue and applications while holding cost of IT operations flat

Reduced time to market for new insurance products by over 50%

These are a few examples from the hundreds of companies that use the Delphix Dynamic Data Platform to fuel their transformation