

How Much of Your Enterprise Production Data Is at Risk in Lower Environments?

More copies. More exposure. Greater risk.

Risk multiplies when sensitive information is copied into development, testing, staging, analytics, or AI...

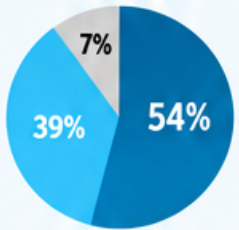
Production Database Data is Pervasive in Development and Testing

Redgate's State of the Database Landscape research found that **54%** of organizations provide full production database backups for development and testing, while **39%** provide subsets of production data.

Only 38% report masking or de-identifying sensitive development and test data, and **16%** report replacing sensitive data with synthetic data.

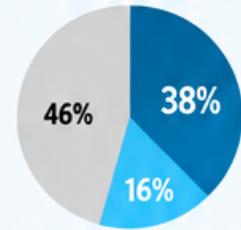
60% of developers continue to use production data.

Development and Test Data Source (Redgate 2025)



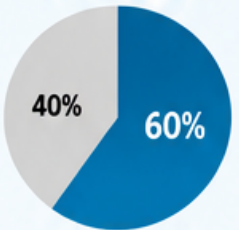
- Full production backup
- Production subset
- Other

Approach to Sensitive Dev/Test Data (Redgate 2025)



- Masking / de-identification
- Synthetic data replacement
- Other

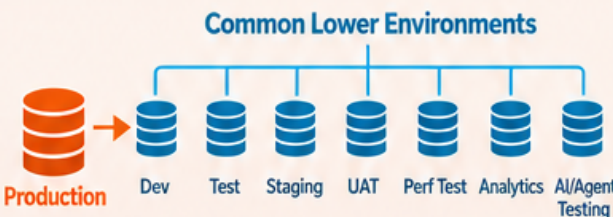
Developers Using Production Data (IDC via Redgate)



- Use production data
- Do not use production data

One Production Dataset. Many Copies. A Growing Attack Surface.

Sensitive data is routinely replicated across multiple non-production environments. Each copy creates another location that must be discovered, governed, secured, and ultimately removed.



45% maintain 3 or more non-production copies of each production dataset.

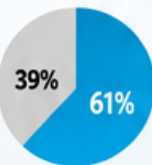
- 54% maintain 1–2 copies
- 42% maintain 3–6 copies
- 3% maintain 7–10 copies
- <1% maintain more than 10 copies

Source: Perforce/Delphix. 2025 State of Data Compliance and Security Report.

Production Document Data Creates Another Major Exposure

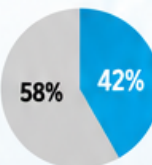
Sensitive production information also moves through active business processes in loan applications, insurance claims, medical forms, financial documents, contracts, PDFs, spreadsheets, images, and other electronic documents.

Experienced Unauthorized Access to Sensitive Information in Files (Ponemon 2025)



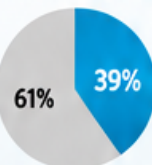
61% of organizations experienced unauthorized access to sensitive or confidential information contained in files within the previous two years.

High Confidence Files Are Secure During Upload (Ponemon 2025)



Only 42% have high confidence that files are secure during the upload stage (e.g., web forms and portals).

High Confidence Files Are Secure When Transferred to Third Parties (Ponemon 2025)



Only 39% have high confidence that files are secure when transferred to and from third parties.

Files Often Contain Personal Data (Verizon DBIR 2025)



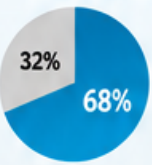
95% of confirmed data disclosures involved personal data, often through misdelivery or improper sharing of documents.

Sources: Ponemon Institute. The State of File Security, 2025. | Verizon. 2025 Data Breach Investigations Report (DBIR), 2025.

The Unstructured Data Challenge

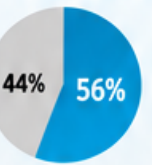
Unstructured data — including documents, emails, images, and other files — contains a significant amount of sensitive information, and most organizations lack full visibility and protection.

Organizations with Unprotected Unstructured Data (Cloud Security Alliance 2026)



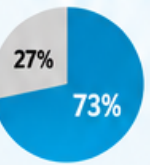
68% report that a significant portion of their unstructured data remains unprotected.

Limited Visibility into Unstructured Data (Cloud Security Alliance 2026)



56% have only partial visibility into where their unstructured data is stored.

Documents and Files Dominate Unstructured Data (Cloud Security Alliance 2026)



Documents and files represent **73%** of unstructured data in the organizations surveyed.

Source: Cloud Security Alliance. The Rise in Unstructured Data and AI Security Risks, 2026.

The Answer - Enterprise Data Provisioning from GenRocket

Protect all data. Expand coverage. Scale with control.

01 | PROTECT



- Secure lower environments
- Mask sensitive data
- Redact documents and files

SECURITY

02 | EXPAND



- Use synthetic data
- Maintain data quality
- Cover structured and unstructured data

DATA QUALITY

03 | SCALE



- Automate and integrate
- Govern and monitor
- Enable AI and innovation with confidence

OPERATIONAL EFFICIENCY

Reduce Risk. Improve Quality. Raise Efficiency



Quality Evolution Platform