Teleran Dynamic Data Masking Advantages

Feature	Description	Teleran Advantage
Simple, Automated Implementation	Simple automated installation and configuration implements quickly and easily.	Reduces complexity and speeds time to protection. Other solutions are complex and require days or weeks to implement.
Automatic Policy Creation	Automatically generates dynamic masking policies and data access policies from Teleran Data Discovery or other data tagging tools.	Saves time. Minimizes risk of human error. Maximizes accuracy of protection policies. Other solutions require manual policy creation and updating that can introduce protection gaps and increase staff overhead and costs.
Integrated with Comprehensive Data Protection Suite	Integrated with Teleran Data Discovery, Auditing, Alerting, Reporting and real-time Access Policy Enforcement.	Provides comprehensive, integrated data protection and compliance solution. Reduces complexity, management overhead and costs. Other vendors offer point solutions or many unintegrated products, increasing complexity, integration effort and costs.
Cloud-Designed Solution	Uniquely architected SaaS solution supports on-premise, hybrid and public cloud environments.	Delivers uniform data protection across all sensitive data independent of data location or future disposition. Other vendors deliver different solutions across on premise and cloud environments.
Fast Performance No Query Latency	Highly performant data masking policy engine. No impact on user experience or response time SLAs.	Supports high demand, high volume environments. Other solutions require more complex processing that introduces latency and impacts performance. Native database solutions such as Oracle Redaction or Microsoft SQL Server/Synapse Analytics Dynamic Data Masking use “ALTER” commands that consume database resources and impact performance.
SaaS Offering	SaaS-based solution simplifies data masking implementation and delivery.	Simple, fast process speeds implementation, reduces complexity, enterprise scalable. Other solutions are complex and require days to install and configure on premise or in the cloud.
Supports all Applications	Highly flexible comprehensive policy engine supports all SQL applications without restriction.	Oracle and Microsoft solutions cannot support business intelligence tools, analytical applications or any ad hoc query tools, leaving sensitive data vulnerable to inferencing or brute force data breaches.
Closes Data Security Gaps Not Addressed by Other Solutions	Closes “ data inferencing” and other data security gaps left open by other solutions.	Prevents users with ad hoc access database tools like business intelligence or analytics from progressively narrowing down successive searches to reveal actual sensitive data. Some native database solutions such as Microsoft Dynamic Data Masking and Oracle Redaction leave real security gaps including inferencing.
Independent of Databases and Applications	Operates outside of the database. Requires no changes to data model or application code.	Simple, extensible product architecture speeds time to protection, reduces complexity. Native database solutions such as Oracle Redaction require integration with applications and scripting.
Business-Context Aware Data Masking	Includes user, role, location, application and other business parameters.	Ensures appropriate data masking policies are applied in context of actual business usage, geographic-specific regulations, and application behavior. Other solutions do not leverage business context, reducing protection.
Business-Oriented No DBA Skills Needed	Offers easy-to-use business-oriented GUI. Supports “Separation of Duties” required by privacy compliance regulations.	No dependence on DBA’s to establish and maintain data masking policies. Ensures compliance requirements are met. Native database redaction or masking solutions require DBA skills.