teleran

Dynamic Data Protection and C

DISCOVER, AUDIT, MASK AND PROTECT SENSITIVE DATA

in Azure, Hybrid and On Premise

KEY FEATURES

Discovers and categorizes sensitive data

Enforces sensitive data masking and data access policies in real-time

Automatically creates real-time data masking and access controls

Audits user, application, query and data usage activity

Closes inferencing and brute force security gaps left open by Azure SQL and Synapse Analytics

KEY BENEFITS

Improves accuracy, cost-efficiency and productivity with automated processes

Prevents data breaches and compliance violations

Integrates with SIEM and other compliance and security systems

Deploys quickly and easily across Azure, on premise and hybrid environments

For more information visit

http://www.teleran.com

or call +1.973.439.1820

Sensitive Data Discovery, Auditing, and Protection Controls

Teleran's Data Protection and Compliance solution offers three key components. It discovers sensitive data such as personal identifiable information (PII) on premise, in Azure and hybrid database environments. It provides auditing of that sensitive data access, identifying the "who, what, where, when, and how" of each transaction. It also delivers sensitive data masking and real-time data access controls that prevent unauthorized or suspicious activities by authorized users and potential hackers. Teleran's solution addresses data protection regulations like PCI, HIPAA, California Consumer Privacy Act, GDPR and others.

Microsoft Azure Certified

Comprehensive Data Protection and Compliance Solution

- **Automated PII Discovery** identifies sensitive data in databases related to leading data privacy regulations
- **Automatically Creates Sensitive Data Masking and Access Control Policies** integrated with Discovery process
- **Continuous Auditing** tracks PII access by user, query, and application
- **Patented Real-time Policy Action Engine** dynamically masks sensitive data or prevents inappropriate and non-compliant data access
- **Closes Azure SQL Database/Synapse Analytics Security Gaps** by preventing inferencing and brute force attacks
- **Automated Alerting** communicates warnings to security and compliance staff
- **Network-Proxy Listener Agent** installs quickly and requires no performance degrading "in-the-database" agents, traces or monitors