teleran
Data Protection and Compliance

SOLUTION
WHITE PAPER

Discover, Audit & Protect Sensitive Data

On Premise and in the Cloud

BENEFITS

Improves accuracy, cost-efficiency and productivity with automated processes

Minimizes risks of data breaches and compliance violations

Automates policy generation saving time and ensuring maximum protection

Integrates with SIEM and other compliance and security systems

Deploys quickly and easily

KEY FEATURES

Discovers sensitive PII data

Automatically creates real-time data masking and access controls policies

Audits user, application, query and data usage activity

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

Alerts staff in real-time to threatening or suspicious behavior

Teleran Data Protection and Compliance Software

Highly damaging and widely publicized data breaches are occurring with greater frequency. Regulations such as GDPR, PCI, HIPAA/HITECH, the California Consumer Privacy Act and others are driving up the cost of compliance and increasing the financial penalties associated with data breaches and compliance violations. Breaches are continuing to grow despite large investments made in perimeter and network security solutions.

These solutions alone are not sufficient to protect organizations from potentially devastating data breaches and costly penalties. Organizations now must address escalating data risks and regulatory compliance mandates by focusing on protecting sensitive data on premise and in the cloud.

Comprehensive Data Discovery, Audit, Analytics, and Real-Time Controls

Teleran's patented software solution delivers a centralized platform for sensitive data discovery, auditing, compliance reporting, analysis, real-time alerting, dynamic data masking, and data access controls.

Teleran's data protection and compliance solution continuously discovers, watches, analyzes and controls how sensitive data is accessed, by whom, in what business context, and with what applications. Its granular, context-sensitive policy enforcement blocks inappropriate queries before the database is even reached. It dynamically masks sensitive data before it leaves the database. Teleran offers organizations an integrated data protection and compliance solution that safeguards their critical data quickly and effectively.

Discovering Sensitive Data, Automatically Generating the Appropriate Protection Policies

Sensitive Data Discovery

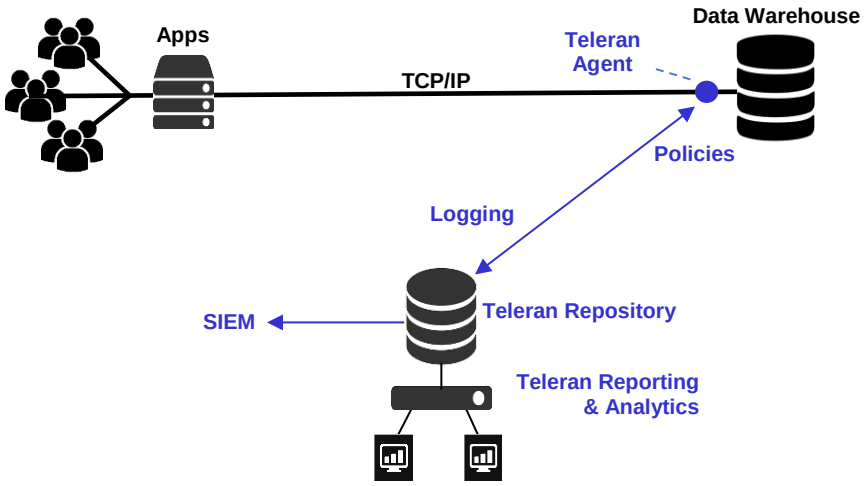
Teleran's solution automatically interrogates databases, identifying and evaluating all database objects to discover what data is sensitive. This process uses regular expression libraries that have been developed for leading commercial applications as well as for common data privacy regulations around the world. Teleran's real-time policy manager is integrated with the discovery process and automatically creates sensitive data masking and access control policies.

Continuous, Unobtrusive Auditing of Sensitive Data

Continuous Auditing

Teleran's continuous and unobtrusive monitoring captures 100% of user and application traffic without putting overhead on the databases. Its patented network agent monitors at the database network protocol layer, delivering complete visibility of sensitive data access across your environments without interfering with internal database processes or slowing performance.

Teleran captures and controls usage at the network layer on premise or in the cloud.



Database applications today are used by a wide array of organizations. As a result, sensitive data is potentially exposed across a complex array of data infrastructures on premise and in hybrid and public clouds. Because of this exposure, monitoring not only at the data layer, but also across users and applications is critical.

Teleran's solution identifies who the actual user is, his or her organizational context, the application in use, the SQL query launched by the application and the data accessed. It also tracks privileged user activity including data manipulation (DML) such as inserts, updates, deletes, and other database maintenance activities such as granting permissions, and adding and deleting tables

Ensuring All Users Are Identified, Profiled and Controlled

It is critical to know who your users really are to identify who is generating inappropriate queries or accessing sensitive data or whose credentials have been compromised. But most applications mask the user identity to the database by using connection pooling, Active Directory, LDAP or generic database IDs. So if you are just monitoring at the database, you can't determine who is doing what. iSight's patented Identity Persistence™ feature associates the authorized user with the actual query that gets processed by the database. It ensures the user's identity is not lost, guaranteeing the effectiveness of Teleran's user behavior analytics, incidence response, and query control policies.

Integration with Applications Builds Deeper Context and Protection

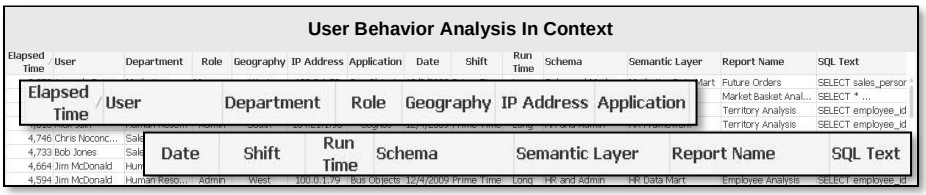
It is not only important identify and track contextualized user activity. It is also critical to understand how users are interacting with the applications they are using, and putting that together with what is happening at the data layer. Teleran's solution deploys several patented methods to unobtrusively capture application level metrics including application user ID, application names, report names, application server activity, and in the case of leading BI and analytical applications, semantic layer activity.

With this context you now have deeper visibility, across users, applications and database activity, to establish effective user behavior profiling, rapid threat detection and response, comprehensive reporting as well as more effective real-time user and query controls.

Contextualized Auditing Delivers Deeper Insight and Control

Teleran also delivers Business Context™, a critical capability that associates users with their specific organizational context, including dimensions such as location, geography, role, and functional area or department. This enables deeper insight and context for profiling expected user behavior, identifying malicious or inappropriate behavior, and delivering actionable real-time alerts and user controls without impeding users' legitimate data access and business process.

Teleran's contextualized auditing delivers a comprehensive picture of user, organization, data, application, and transaction activity.



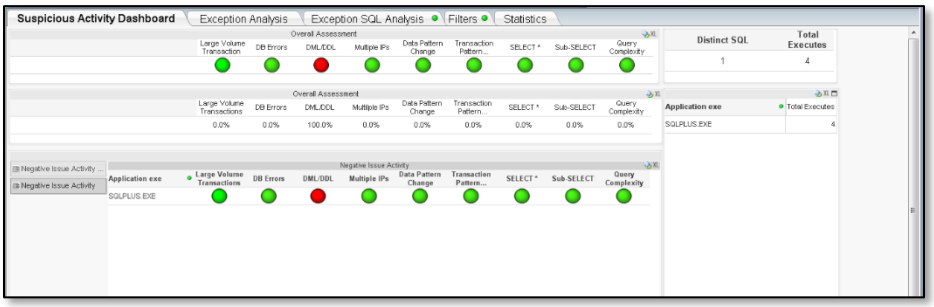
Analytics Detect Suspicious and Malicious Behaviors

User Analysis & Alerting

Teleran's solution delivers sophisticated analytics as a foundation for data protection and compliance. It identifies threats such as SQL injection, malicious insider behavior, and suspicious data usage patterns.

Teleran's User Analytics profiles user behavior identifying normal and exception behavior across a range of data activity including DML, DDL, DCL, and read only activity such as SELECTs and stored procedures. It automatically detects material changes to user behavior, triggering an alert for further investigation or directly blocking the user access. It also provides near real-time reporting, providing incidence response teams with visibility into activity as it is occurring. In addition, Teleran's solution provides forensic analysis over time to identify subtle malicious user behaviors that may not be immediately apparent.

Teleran's iSight Analytics identifies malicious or suspicious behaviors.



Alerting Drives Appropriate Action and Remediation

Alerts tied to threat detection as well as suspicious user behavior direct immediate and targeted incidence response. Alerting and forensic information can be automatically sent to SIEM, SPLUNK or other solutions and integrated with broader remediation workflows.

Real-time alerts drive immediate and appropriate remediation.

From: iGuard Alert [mailto:501458408@chicisapp429v.corporate.gr.com
Sent: Monday, January 23, 2019 3:23PM
To: rsimon@gr.com
Cc: security1@gr.com
Subject: iGuard Daily Status for 01/23/19
Exception activity: large data set queries above profile threshold trending over 3 day period from finance.

Real-Time Data Masking and Access Controls Protect Data

Dynamic Real-Time Controls

Teleran's real-time policy management solution delivers control policies that automatically protect sensitive data from malicious or unauthorized access. Policies include:

- Sensitive data redacting
- Sensitive data object access blocking
- Database connection white/black list
- Data manipulation restrictions (DML/DDL)
- User/application white/black list
- Joins and other SQL restrictions

With an easy-to-use wizard, compliance staff apply or to enforce real-time data masking and granular data access controls.

Sensitive Data Access Policy

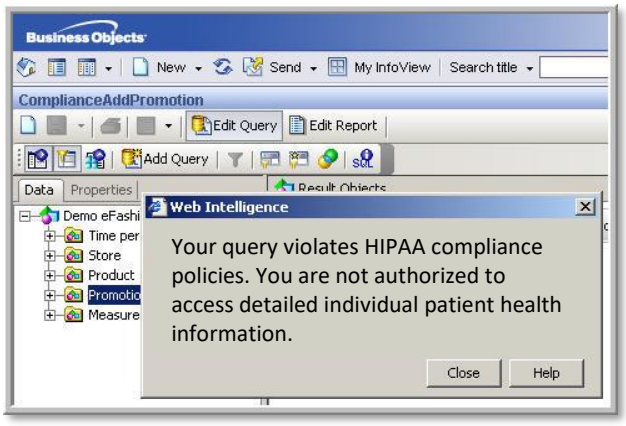
Sensitive Column Restriction	Prevent and/or alert on queries accessing <TABLE> if query contains <SENSITIVECOLUMN> by <USER> and <DATASOURCE>.	Use this policy to prevent/alert access to sensitive columns.

Sample End-User Report with Sensitive Data Masked

EMP Name	SSN#	Role	Annual Salary	Location
Phil	XXX-XXX-XXXX	ASE	$9999999999	Palo Alto
Liam	XXX-XXX-XXXX	AE	$9999999999	Boston
Sarah	XXX-XXX-XXXX	SE	$9999999999	New York
Rich	XXX-XXX-XXXX	PR	$9999999999	Atlanta

All policies can be applied by users/groups, functions, departments, geographies, applications, and data objects down to the column level. Active policies screen information requests before they reach the database, block those that violate policies, and if appropriate, issue messages to application users warning them of their attempted violation.

Messages warn application users of attempted compliance policy violations.



Automated Protection Policy Generation

Automated Policy Generation

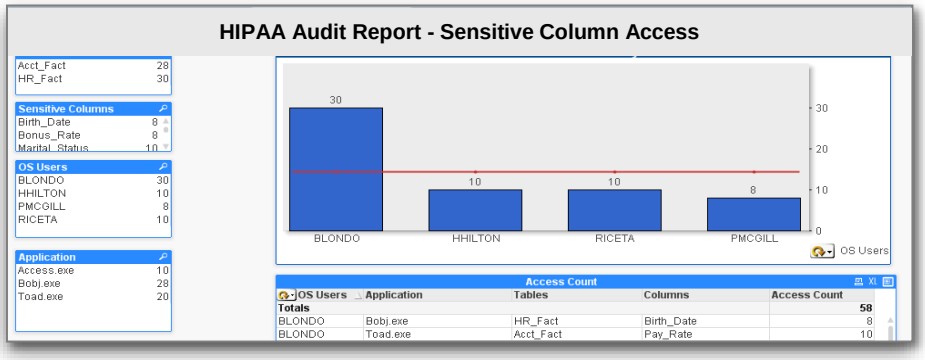
Teleran's policy management system is integrated with Teleran's Sensitive Data Discovery process. It also can receive sensitive data tagging from other discovery solutions. Once data is tagged as sensitive, the policy manager automatically generates the appropriate access and redacting policies that can then be applied by user, groups, and applications. Automatic policy generation saves time and ensures policies are effective and up to date with changing data, users and applications.

Automated Compliance Reporting for Non-Technical Staff

Compliance Reporting

Teleran's solution delivers out-of-box compliance reports that address GDPR, PCI, HIPAA, and many other regulatory requirements. Automated compliance reporting enables compliance and data protection staff to immediately be productive while reducing audit costs and risks. Teleran's customizable reporting system is designed for use by non-technical roles including auditors and compliance professionals and establishes clear separation of duties as required by compliance regulations.

HIPAA Compliance Audit Report highlights sensitive columns access exceptions.



Fast Time-to-Value

When it comes to data protection and compliance, organizations can no longer risk long and expensive implementation cycles. Teleran's Data Protection and Compliance solution automates installation and configuration processes for rapid deployment. This enables you to deliver fast time-to-value with minimal effort.

Flexible Deployment and Licensing Options

Protecting sensitive data wherever it resides is critical to meeting today's data risks and compliance requirements. Teleran's scalable and flexible product architecture enables organizations to protect their database applications on premise, in hybrid cloud deployments as well as in leading public clouds. Teleran offers flexible licensing and deployment models including software subscriptions, perpetual licensing, and managed services.

Contact Us

For more information about Teleran's Data Protection and Compliance Solution visit www.teleran.com or call us at +1.973.439.1820.