PROTECT AND AUDIT SENSITIVE DATA

Teleran Data Security and Compliance

KEY FEATURES

Monitors user, application, query and data usage activity

Enforces data access policies in real-time

Alerts staff in real-time to threatening or suspicious behavior

Establishes detailed user, application and organizational context

Delivers out-of-the-box compliance reports

KEY BENEFITS

Minimizes risks of data breaches and compliance violations

Accelerates threat detection and incidence response

Provides audit, security analytics and access controls in one system

Automates incidence response and data protection

Integrates with SIEM and other compliance and security systems

Deploys quickly and easily

Highly damaging and widely publicized data breaches are occurring with greater frequency. In addition, regulations such as PCI, Dodd Frank, HIPAA, EU General Data Protection Regulation (GDPR) and others are driving up the cost of compliance and increasing the financial penalties and sanctions of data breaches. 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 the data where it lives – in the database.

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

Teleran's patented software solution delivers a centralized platform for auditing, security analytics, user behavior analysis, real-time alerting, data access policy enforcement, and compliance reporting.

Teleran's data security and compliance solution continuously 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

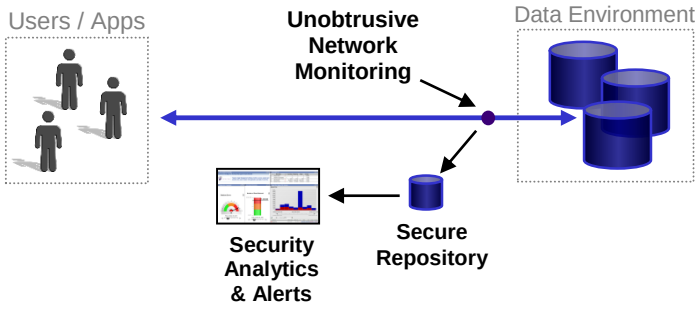
reached. Teleran offers organizations a best-in-class data security and compliance solution that safeguards their critical data quickly and cost-effectively.

Continuous, Unobtrusive Monitoring of Sensitive Data

Real-Time Data Monitoring

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

Teleran's solution captures usage traffic at the network layer.



Database applications today are used by a wide array of business roles, functions, applications, and geographies, both internal and external to organizations. As a result, sensitive data is potentially exposed across a complex and large data ecosystem. Because of this exposure, it is critical to monitor, not only at the data layer, but also across users and applications as well.

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 data manipulation (DML) activity including inserts, updates, deletes, and other database activities such as granting permissions, and adding and deleting tables

Ensuring All Users Are Identified, Profiled and Controlled

User Identity & Business Context

It is critical to know who your users really are to identify who is generating inappropriate queries or accessing sensitive data. But, most applications mask the user identity to the database by using connection pooling, single sign-on/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 business 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 security and user behavior analytics, incidence response, and query control policies.

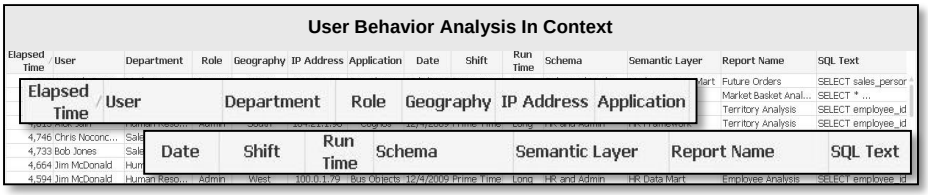
Contextualized Auditing Delivers Deeper Insight and Control

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.

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 Application Context™ 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. Now you have the deeper context, 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.

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



Security Analytics Detect Threat and Malicious Behaviors

Security Analytics

Teleran's solution delivers sophisticated security analytics as a foundation for data security and compliance. It automates threat detection such as SQL injection, malicious insider behavior, and suspicious data usage patterns. Teleran's Security Analytics profiles user behavior, establishing baselines for 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 both real-time, 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.

Alerting Drives Appropriate Action and Remediation

Real-Time Alerting

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

Real-time security alerts drive immediate and appropriate remediation.

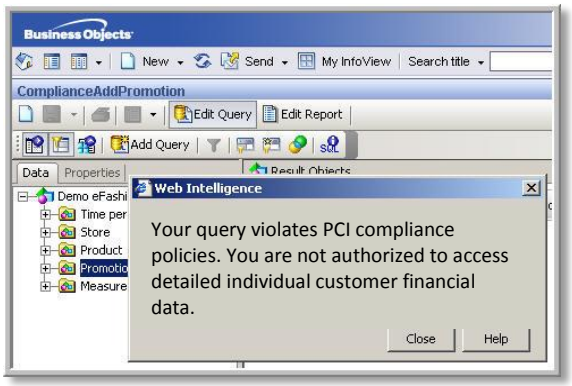
From: iGuard Alert [mailto:501458408@chicisapp429v.corporate.gr.com
Sent: Monday, January 26, 2016 3:23PM
To: rsimon@gr.com
Cc: security1@gr.com
Subject: iGuard Daily Status for 1/26/16
Exception activity: large data set queries above profile threshold trending over 3 day period from finance.

Automated Policy Enforcement Protects Sensitive Data in Real-Time

Real-Time Data Access Controls

Teleran's Data Security and Compliance solution delivers access policies that automatically protect senstive data from malicious or unauthorized reports and queries. With an easy-to-use wizard, compliance staff define, test and enforce real-time data access policies. Policies can be applied to specific SQL injection signatures, users/groups, functions, organizational groups, geographies, applications, and data objects down to the column level. Active policies screen information requests from users and applications before they reach the database, block those that violate policies, and if appropriate, issues messages to application users warning them of their attempted violation.

Messages warn application users of attempted compliance policy violations.



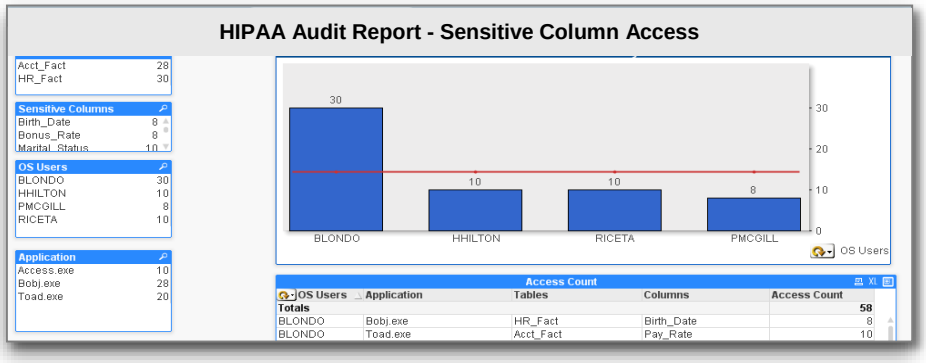
teleran

Compliance Reporting

Automated Compliance Reporting for Non-Technical Staff

Teleran's solution delivers out-of-box compliance reports that address PCI, Dodd Frank, HIPAA, EU General Data Privacy Regulation (GDPR) and many other regulatory requirements. Automated compliance reporting enables compliance and security 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 security and compliance, organizations can no longer risk long and expensive implementation cycles. Teleran's Data Security and Compliance solution automates installation and configuration processes for rapid deployment. This enables you to deliver fast time-to-value at a reasonable cost.

Flexible Deployment and Licensing Options

Protecting sensitive data wherever it resides is critical to meeting today's security 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 Security and Compliance Solution visit www.teleran.com or call us at +1.973.439.1820.

teleran