INTRODUCING **DATASKOPE**

Empowering Data Security and Compliance: Your Ultimate Database Activity Monitoring Solution.

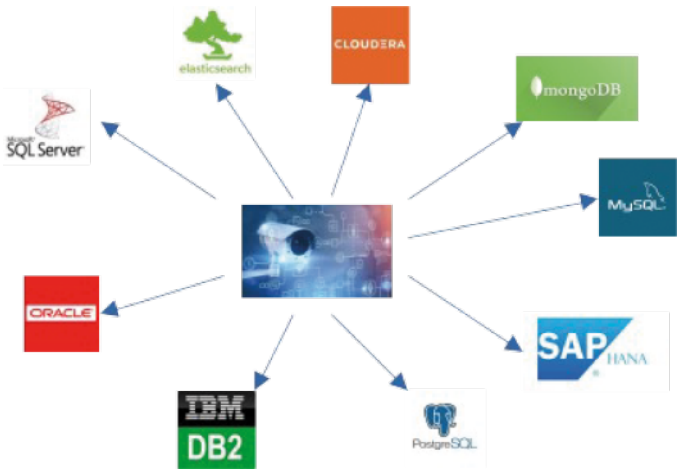
WHAT IS **DATASKOPE?**

Dataskope monitors any activity happening to all your databases and can help you detect and take action to prevent malicious tempering of your most personal and sensitive data.

Dataskope records all activities and provides reporting and analytics to fulfill your auditing and compliance requirements.

Privileged user and application access monitoring is accomplished independently from native database logging and audit functions (performance).

It can function as a compensating control for privileged user ensuring separation-of-duties by monitoring administrator activity.



Why do you need to closely monitor your databases and instantly prevent data breaches?

Databases are at the heart of every business application. They store critical, personal, and sensitive information. Companies in general have to manage a number of heterogeneous database technologies to accomplish all tasks they need for their business to be successful. Databases are accessed by a multitude of users and applications, coming from disparate sources and running diverse queries.

The Auditing and recording of database activity plays an essential role in achieving data privacy laws compliance: This ongoing exercise is a mandatory requirement from: ie GDPR, HIPAA, SOX, PCI. Companies need the ability and ease to perform monitoring of constant solicitation to their databases but also prevent data breaches through detection of unusual activity.

Several crucial problematic questions are rising in your security officer's mind that urgently need appropriate answers:

- How can I track unauthorized/unplanned access to database systems?
- How can I track and monitor developers' and DBAs' activities on production systems?
- How can I track access to sensitive and personal information?
- Who accessed this personal and sensitive column in these heterogeneous databases?
- Did the same intruder connect to these heterogeneous databases?
- Can you identify anomalies in activities?
- What queries were sent by this user?
- What queries were sent by this application?
- Who updated this column in these heterogeneous databases? and when?
- Is the connected user legitimate?
- Can you prevent a particular access to a particular database table?
- Can you detect an illegitimate access?
- Would illegitimate access be reported immediately?
- Can you abort it?

The list of questions can grow and become overwhelming.

What benefits do you receive using Dataskope?

Dataskope monitors database activity without requiring audit subsystem of the respective RDBMS server being turned on: a huge performance benefit. It classifies and correlates the audit logs and stores them outside the database complying with separation-of-duties principle and enabling analysis across heterogeneous databases. It ensures that a service account can access a database only from a defined source, and only runs a narrow group of authorized queries. This can be used to detect "compromises of a service account" either from the system that normally uses it, or if the account credentials show up in a connection from an expected system.

Dataskope agents can record all SQL statements (DML, DDL, DCL, and TCL) without relying on local database logs, thus reducing performance degradations.

What are the main features of Dataskope?

Monitor logins: monitor successful and failed logons and ensure they are from predefined and valid legitimate sources.

Monitor changes: monitor and audit all DML, DDL, TCL and DCL commands (SELECT, UPDATE, DELETE, EXEC, and other SQL statements).

Monitor access to sensitive information: monitor who is accessing sensitive information. When the unexpected happens generate alerts and/or prevent it from happening.

Monitor privileged users: audit dba/developer activity and configuration changes to the database system.

Generate reports, and dashboards, Perform analytics and M/L: predefined policies and reports for GDPR, PCI DSS, SOX, KVKK or any similar 'data protection and privacy compliances' applied in your country requirements; highlighting "data product" consumption, derived from the activities using analytics and M/L.

What performance and scalability can you expect from Dataskope?

Dataskope is an enterprise grade solution developed with scalability in mind. It can be deployed on physical or virtual machines with no storage or hardware limitations.

You can add more resources as your needs grow.

What operating systems does Dataskope support?

Dataskope server runs on windows and soon on Linux. Dataskope agent is written in C++ and can run on all major operating systems such as Windows, and Linux/Unix distros (example: Redhat, Suse, AIX, Solaris)

What database systems does Dataskope support?

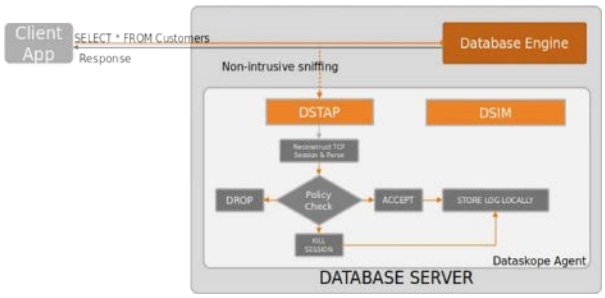
All major RDBMS products are supported: MS SQL SERVER, Oracle/Exadata, Teradata, DB/2, MySQL, PostgreSQL, etc.

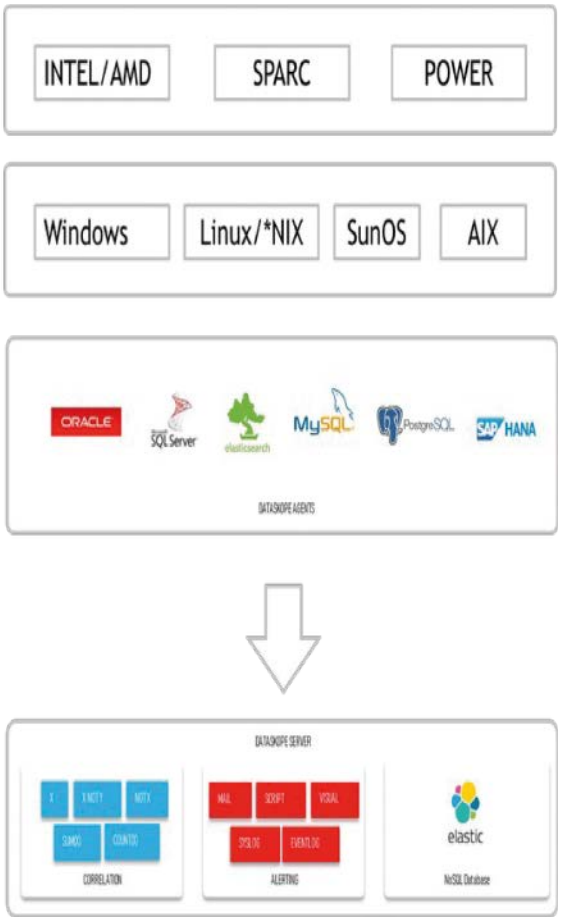
A number of Big data solutions are supported: MongoDB, Cloudera, ElasticSearch.

How does a Dataskope agent work?

Agents monitor network traffic to capture queries. Local activities such as Oracle Bequeath connections are also monitored and captured.

Dataskope agents will not cause any service outage since they do not work as a middle-man, therefore as a single point of failure risk.





What security features does Dataskope offer?

Dataskope server runs on a hardened Windows server or Linux box you own. Unlike other systems, no password is hidden from you, you have all the passwords to login to Dataskope server and perform maintenance tasks. Every audit record is stored with a hash value to provide log integrity.

Dataskope supports local and LDAP authentication as well as role-based-authorization to ensure logs can only be viewed by an authorized operator. You can determine who-can-see-what as well as who-can-do-what. All operator activities are also logged.

How does Dataskope ensure confidentiality?

Dataskope can recognize and mask sensitive/personal information (credit card numbers, email addresses, medical records, etc.). Recognizers can be extended and configured via regular expressions.

Dataskope comes with built-in user id chain detection that lets you discover the actual user behind "runas", "su", and "sudo".

A sophisticated complex-event-processing-engine enables you to correlate, search, define log collection policies and alerts.

```
action_type:        query
auth_machine:       localhost.localdomain
auth_pid:           4117
auth_program_nm:    ********************domain (TNS V1-V3)
auth_sid:           oracle
auth_terminal:      pts/1
capture_type:       parse
client_app_name:    java
client_flags:       3
client_hostname:    localhost.localdomain
client_ip:          127.0.0.1
client_platform:    x86_64/Linux 2.4.xx
client_port:        53554
client_protocol_ver: 6.5
correlation_id:     3e13f276-cb1a-4bab-aadf-b1732663aa18
db_protocol:        TCP
db_type:            oracle
db_user:            SYSTEM
execute_options:    32865
os_user:            oracle
params_count:       0
port:               1521
query:              select * from dual where 1=1**********4
query_len:          114
result:             Completed
```

Can Dataskope detect malicious intrusion and prevent it from doing harm?

Dataskope offers a sophisticated set of policies to enable detection of unusual activity or unauthorized connection. Upon detection of such event, Dataskope can abort the activity and kill the connection, and also send alerts.

ALERT
INTRUSION DETECTED

Feature	DS
Windows Support	✓
Linux support	✓
Agent can audit client application	✓
Agent can audit application server	✓
Agent can audit database server	✓
Scalable architecture	✓
Distributed architecture	✓
Integrated with LDAP	✓
Integrated with SIEM products	✓
Role based authorizations	✓
Masking of sensitive information	✓
API support	✓

GET IN **TOUCH**

Phone: +90 (212) 924 2030 **Mail:** info@kafein.com.tr **Web:** www.kafein.com.tr

kafein technology solutions