datiphy™

SOLUTION BRIEF
Data Behavior Analytics — DBA

THE CHALLENGE

Perimeter and Network Security tools lack visibility into the data activities, which leads to lateral east-west originating threats against critical business data assets.

SOLUTION BENEFITS

- Identify, classify, and track regulated or sensitive data within databases and tie all activity to the exact origination of data access
- Real-time actions can be taken based on behavioral analysis and audit results
- User-configurable content rules that meet regulations relating to personally identifiable information (PII), protected health information (PHI), and credit card information
- Assesses, monitors, and alerts security permissions for users, administrators and developers
- Real-time analysis of intrusions in the database environment, with full forensics recording for post-mortem analysis of unusual behavior
- Integrated event analysis with other network tools, such as SIEM, for a more comprehensive security framework

A significant problem enterprises face is data visibility and containment. A rogue database server running since the application development cycle may become a threat vector. This could be a structured or unstructured database running on-premise or in your hybrid cloud infrastructure. Discovering, classifying, protecting, and documenting all business data assets is paramount to breach detection and data protection.

It's widely agreed that it's not if, but when a database breach will occur. The database was the primary attack vector in the majority of data thefts. Malicious actors are able to mask themselves to go undetected by the firewalls, IPS (intrusion prevention systems), and endpoint security solutions. Information security will always require a multi-tiered approach — no single tool will eliminate all the vulnerabilities.

Behavioral analysis is being applied to network traffic and users, while little focus has been placed on the data itself. End-to-end Database Behavior Analytics (DBA) provides a vastly different context into your business and data activities. Your business is completely dependent on data, so hearing the data's story from the actual data is your best line of defense.

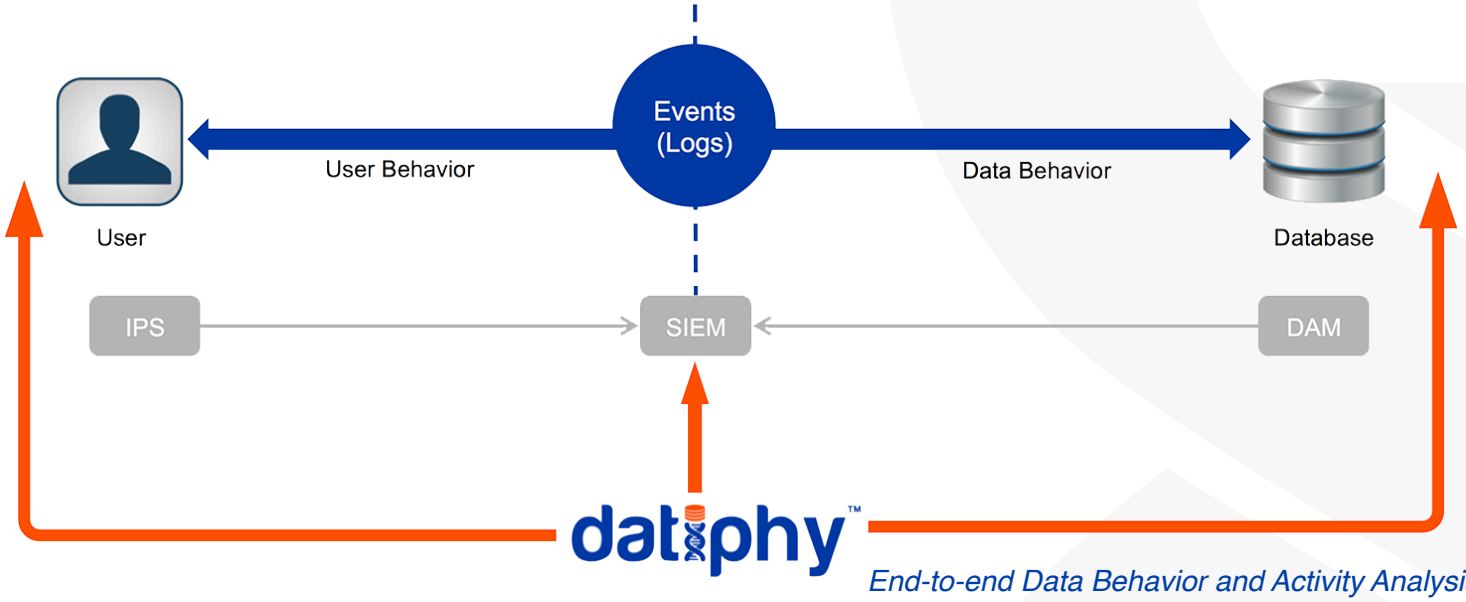
DISCOVERY

The timeless thought – "you can't protect what you can't see" – remains true and couldn't be more applicable to today's ever-changing cyber world. Information overload is leading to a lack of visibility, resulting in enterprises essentially searching through the dark when trying to track down a database breach. Big data and information overload amplifies this and organizations seeking a competitive advantage require a solution like DBA to truly monitor everything.

The only way you can protect against database threats is learning the normal behavior of your data and then look for deviations to that known behavior. How your web application users connect to the database servers is highly valuable to detecting a compromised application. How an application server talks to the database is equally as valuable. A privileged user, like a DBA, App Developer, or DevOps Engineer, looking at large amounts of customer data when he's never accessed that particular database server before could be a compromised user.

CLASSIFICATION

After identifying all the databases in an environment, you can start classifying the databases that house sensitive data. Predefined deep content filters and user definable content discovery attributes to find a variety of sensitive data types such as credit cards numbers, social security and drivers license information, medical records, bank accounts, or passport numbers.



End-to-end Data Behavior and Activity Analysis

Security professionals will be able to define their own custom data patterns to monitor. Identification is not just limited to the database itself, it also involves the precise location of sensitive data – database, table, and column level visibility.

After sensitive data has been identified, the next major step is to track and analyze all user behavior. This could be your Web Application Users, Database Administrators, Application Developers, or DevOps Engineers. Specifically what must be monitored is the user behavior around access of sensitive data. That is the blurry cross section of authorized and unauthorized behavior.

PROTECTION

Once the landscape is defined, protecting it is a little bit more manageable. Centrally managing privileges and controlling access is just one component of protection. Learning the behavior and then discovering dynamic changes within the environment is key. Compromised user accounts or inside abusers will most often be the primary attack vector. In this case the user is completely authorized to access the database, however, this malicious actor will perform some behavior that is different than the standard user. Separation of duties violations is another key monitoring point – i.e. when an unauthorized IP subnet accesses the database.

SQL injection has been a common attack vector for the last 10 years, and likely always will be. Applications will always have vulnerabilities. If an application typically queries a database for credit cards at predefined intervals, let's say one credit card per query, then policy and alerting can be setup around excessive credit card access. This is a common indicator of an application hijacking via SQL injection. A real application user dumping the contents of the entire database in a single query could be another SQL injection attack.

Not only detecting the breach, but also having the forensics evidence and data trail behind the breach allows the loop to be closed. Many times enterprises and government agencies struggle with the damage caused by a breach — typically leading to embarrassment, loss of brand reputation, and even revenue. Having all the data evidence at your fingertips allows for optimal operational efficiency. With data growing faster than the perimeter, a data-centric approach crosses silo boundaries providing uncompromised visibility throughout physical and cloud environments.

ABOUT DATIPHY

The Datiphy platform fills the gaps that exist between point solution tools and glues various capabilities together to visualize your entire enterprise data lifecycle. The key technology is its Adaptive Data Behavioral Model™ (also called DatiDNA™) providing the scientific certainty of analyzing the entire data pool as events occur in real-time. A command portal enables centralized management and natural language queries empowering users to find any data asset within seconds and see the context of every interaction that has occurred among all other assets.

For more information about the Datiphy Platform or to schedule a product demonstration please visit www.datiphy.com

datiphy™

ADDRESS
2290 N. First Street, Suite 204
San Jose, CA 95131

WEBSITE
www.datiphy.com

SALES
sales@datiphy.com
+1.888.343.9938