Universal User Tracking
Auditing and User Accountability

Do you know who is accessing your sensitive database data? Business mandates and compliance requirements are driving organizations to audit all database activity. Database audit trails must include the individual SQL query, the database response, the timestamp, and, most importantly, the individual user that accessed or changed database data. Unfortunately, for many multi-tier applications, it can be difficult – if not impossible – to identify the end user from database transactions alone.

Imperva has developed multiple methods to accurately identify end users regardless of how these users access the database. Imperva's Universal User Tracking supports architectures that use connection pooling to aggregate multiple user sessions into a single database connection. Universal User Tracking tracks end users without requiring any changes existing databases, applications, or network. Universal User Tracking supports enterprise applications, such as Oracle E-Business Suite, SAP, PeopleSoft, J.D. Edwards, and Siebel, as well as custom and internally-developed applications. With Universal User Tracking, organizations can identify the actual end users that accessed their most sensitive information: customer, employee, and financial data.

By tracking application and database users, SecureSphere can display user IDs in security alerts, audit logs, and reports. In addition, SecureSphere can dynamically profile user activity to establish a baseline of acceptable behavior per user. And security policies can be created to restrict access by user ID. Tracking end users enhances security and improves visibility into database and web application activity.

Universal User Tracking consists of two overarching user identification methods: Application User Tracking and Direct User Tracking. Application User Tracking tracks users that connect indirectly to the database through an application. Application User Tracking options include Web Application User Tracking, Web to Database User Tracking and SQL Connection User Tracking. On the other hand, Direct User Tracking, as the name implies, tracks users that connect directly to a database through a standard SQL client.
Application User Tracking

- **Web Application User Tracking** leverages Imperva’s expertise of web technology to recognize when users login to an application. By associating a session ID, such as a cookie or session parameter, with a user name, SecureSphere can track all web activity by user name.

Web Application User Tracking enables SecureSphere to recognize the individual application users that perpetrated malicious attacks. In addition, SecureSphere can be configured to monitor or block individual application users.

SecureSphere automatically learns the login pages and authentication form fields of protected web applications. This automated learning is based on several criteria, such as keywords on the login page, keywords on the successful or failed results page, and when an application sets a session cookie. SecureSphere customers can verify that the automatically-learned information is correct or edit the User Tracking settings.

Once the learning process is complete, SecureSphere will dynamically track every user login. SecureSphere will bind the user ID with the corresponding HTTP session token. This allows SecureSphere to track the application user throughout the HTTP session.

- **Web to Database User Tracking** combines Web Application User Tracking with the ability to simultaneously monitor web and database traffic to identify which web users performed which SQL transactions. Web to Database User Tracking analyzes the exact time and order of SQL transactions and compares this information with other elements, such as the individual URLs requested and parameters in SQL queries to accurately identify end users.

Web to Database User Tracking enables organizations to audit database activity by end user, even for multi-tier applications that employ connection pooling. And Web to Database User Tracking requires no changes to the existing infrastructure: no application recoding, no domain controller reconfiguration, no agent installation. Web to Database User Tracking offers a fast, easy way to track web application users that access sensitive databases.
- **SQL Connection User Tracking** is an alternative way to audit database users that connect through multi-tier applications. SQL Connection Tracking extracts user IDs from SQL queries to identify users. Some business applications, such as SAP, include the user name in every relevant SQL query. Other applications send a login query that identifies the user immediately preceding a set of SQL queries. And applications like Oracle E-Business Suite use a combination of both methods to tag the application user in the SQL transaction.

SQL Connection User Tracking is the ideal tracking mechanism when user IDs are included in SQL queries. SQL Connection User Tracking can track users regardless of authentication method to either a web or an application server. Web to Database User Tracking, on the other hand, only supports web-based architectures. Web to Database User Tracking also requires monitoring web and database traffic simultaneously from a single SecureSphere appliance.

**Direct User Tracking Options**

Direct User Tracking is the most basic type of user tracking, relying on the native database authentication mechanisms. Direct User Tracking records the database user ID, hostname, IP address, and operating system name of the user directly accessing the database. When users login directly to a database through a dedicated connection, SecureSphere associates the user ID, hostname, IP and system name with all subsequent SQL transactions performed by the user.

Direct User Tracking is primarily used to audit local access by DBAs and direct user access from thick-client applications. For multi-tier applications, Direct User Tracking also identifies anomalous behavior, such as when the IP address or the hostname of the Application Server changes.

- **Database User ID** is the user name that a user supplies when authenticating to the database. For multi-tier applications, the Database User ID is the name of the application server that connects to the database.

- **Client Device Hostname** is the name of the machine from which database transactions originate.

- **Client IP Address** is the IP address of the machine from which database transactions originate.

- **Operating System User Name** is the name of the operating system user that performs database queries. Both Oracle and DB2 databases include operating system user names in database transactions.

**Comparison of Universal User Tracking Methods**

The following table compares the various Universal User Tracking methods and when each method should be used.

<table>
<thead>
<tr>
<th>Universal User Tracking Method</th>
<th>Direct</th>
<th>Web Application</th>
<th>Web to Database</th>
<th>SQL Connection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multi-Tier Applications</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web and Database activity can be monitored simultaneously</td>
<td></td>
<td></td>
<td></td>
<td>Optional</td>
</tr>
<tr>
<td>SQL query or stream includes user ID</td>
<td></td>
<td>Optional</td>
<td>Optional</td>
<td></td>
</tr>
<tr>
<td>Direct Database Access</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
How Universal User Tracking Enhances Auditing and Security

Universal User Tracking is an important element of SecureSphere’s database and web application security and auditing capabilities.

- Monitoring and Alerts. Because of Universal User Tracking, SecureSphere can display the end user ID in all security alerts. User-specific alerts augment understanding of security events and facilitate forensics efforts.

- Audit Logs. SecureSphere records user information in audit trails. Each SQL transaction is accurately associated with an application user. Universal user tracking not only increases the business relevance of audit log messages, but it helps organizations meet today’s stringent compliance requirements.

- Reports. User information included in many pre-defined reports and administrators can generate security and activity reports by user. Universal User Tracking enables granular reports of user access even in connection pooling environments.

- Access Policies. Because SecureSphere tracks both database and application users, administrators can enforce access policies by user ID. Administrators can create custom rules that specify what URLs can be accessed or what SQL queries can be executed. In addition, if a specific security event occurs, SecureSphere can be configured to monitor or block the user responsible for a given period of time.

- User Profiling of Direct Database Users. By positively identifying users, SecureSphere can profile legitimate user activity and, as a result, detect usage anomalies. SecureSphere tracks user names, IP addresses, hostnames and operating system names in its user profile. If a database user performs an unusual database transaction or if a user logs in from an atypical IP address, SecureSphere can generate an alert or block the transaction.

Summary: The Benefits of Universal User Tracking

Imperva’s Universal User Tracking technology makes individual users accountable - even when they access information from multi-tier application infrastructures. By offering multiple user tracking methods, Universal User Tracking can track end users in almost every deployment scenario and application design without requiring application, database or network changes. Universal User Tracking enables organizations to associate changes to financial records or customer data with the specific end user making the change. Because of this, organizations receive greater visibility into database activity, more granular security controls, and adherence to strict compliance requirements.

About Imperva

Imperva, pioneering the third pillar of enterprise security, fills the gaps in endpoint and network security by directly protecting high-value applications and data assets in physical and virtual data centers. With an integrated security platform built specifically for modern threats, Imperva data center security provides the visibility and control needed to neutralize attack, theft, and fraud from inside and outside the organization, mitigate risk, and streamline compliance.