

Application Activity Monitoring - Database Activity Monitoring Services

Traditional network firewalls can be easily subverted by attacks hidden within the application layer, often rendered inaccessible by encryption, lack of analysis depth, or lack of contextual awareness. Web applications mask the real end user web client logons, thus accountability for interaction with data is lost.

Web application security issues are often dealt with by performing encryption and authentication. However, web applications may inadequately judge the appropriateness of database interactions. Anonymous logons, unauthorized manipulation of database structures, stored procedures and data content can easily ruin the integrity of the underlying databases without even gaining unauthorized administrator level access to the database. CGI's Database Activity Monitoring (DAM) service provides a centralized policy enforcement point for the database tier of multi-tiered applications.

Database Activity Monitoring Service

MSS DAM service monitors database activity without burdening the database server. MSS DAM spots unexpected database manipulation, blocks obvious policy violations gracefully, and manages the risks from weak software applications regardless of the software development lifecycle phase. MSS DAM service integrates into the change management processes, and is supported by a service level agreement, delivering 24x7 vigilance and enforcement, without the loss of government policy control.

Basic Services

- Monitoring and Security Exception Handling
 - Vigilant coverage 24x7
 - Identify gross exceptions
 - Low-latency response
 - Notification and recommendation of appropriate containment activities to DBA or client Computer Incident Response Team (CIRT)
- Compliance Information Support
 - Report on granular use of privileged users to data in table space.
 - Report on granular use of application users to privileged data in table spaces.
 - Build user context to support compliance audit trails.
- Duty Separation and Audit Trail Integrity
 - Separate duties such that the database activity logs are immutable and maintained by a trusted third party unmotivated to malicious activity

Optional Services

- Design and Implementation Assessment
 - Identify gaps of application use of databases and application design
- Affirmative Application Service Policy Enforcement
 - Enforce baseline security policy at the database zone perimeter
- Authorized Containment / Intrusion Prevention
 - Owner-authorized database transactions impact
 - Graceful negative acknowledgements to web application servers
- Customized Integration
- Application Security Integration
- Multi-application, enterprise-wide database cluster integration