

DATABASE SECURITY FROM IMPERVA

BENEFITS:

- Alert or blocks database attacks and unauthorized activities
- Identify excessive user rights and dormant user to enable a review cycle
- Audit all access to defined sensitive data using granular control

THE PROTECTION OF DATABASES

The brand any organization is the data that is stored and used. Databases in any organization contain valuable information about the business, their users, and their customers. This type of information is critical to the ongoing existing of an organization, and must be protected. If any of this information was to be leaked out of any organization, the consequences could be harmful if not detrimental to the brand. Securing sensitive business data is a necessity.

DETECTION OF UNAUTHORIZED OR MALICIOUS BEHAVIOR WHILE BLOCKING KNOWN ADAPTIVE PERSISTENT THREATS

Understanding acceptable business behaviors within a network is key to segmenting the appropriate from the unwanted activities. Imperva's SecureSphere Database Security establishes a baseline of all user activity to create normal and acceptable user access patterns within the network. This allows the security application to detect variances when users perform unexpected queries, or attempt to violate access policies. Also, the SecureSphere application monitors all databases in real time to detect unknown data leakage, unauthorized SQL transactions, and protocol and system attacks. Whether the unwanted activity comes from a privileged user or from an adaptive persistent threat, SecureSphere can alert on, quarantine, or even block the attack.

MANAGEMENT OF USER RIGHTS ACROSS DATABASES

Accessing information from multiple databases within an organization is an everyday occurrence. It is vital that organizations find the appropriate balance between access rights to information and protecting data from unnecessary access. The database security component to Imperva's SecureSphere automatically aggregates the users' rights across heterogeneous databases. This can reduce the risk of over or under privileged access rights to users while helping to demonstrate compliance with regulations such as Sarbanes-Oxley (SOX) and Payment Card Industry (PCI).

AUDITING OF SENSITIVE DATA WITH ADVANCED ANALYTICS

Through real time database monitoring, SecureSphere can provide a detailed audit trail providing the "Who, What, When, Where, and How" of each database transaction regardless of the transaction coming from a privileged or non-privileged user. This technology allows for deep insight into activities, and simplifies forensic investigations.

Using Imperva's Database Security component to the SecureSphere security application with Crossbeam's adaptive and high performing architecture provides a solution that addresses all aspects of database security without impacting performance or availability.

ABOUT CROSSBEAM

We improve the sophisticated networks of enterprises, government agencies, and service providers by architecting platforms that are more adaptable, high-performing, reliable, and secure.

