Trustwave®

DATA SHEET

Trustwave User Rights Management

ENSURE DATABASE SECURITY BY LEAST PRIVILEGE

Benefits

- Enable automated and repeatable processes for reviewing user rights
- Identify users with inappropriate or elevated privileges
- Maintain an accurate inventory of database users deployed across the entire enterprise
- Identify valid privileges that may require database activity monitoring
- Provide an accurate audit trail of how a user's rights were assigned
- Meet regulatory mandates that require restricting user access and securing data from inappropriate access.

Job promotions, transfers, mergers and acquisition, role inheritance, or administrative complacence often result in users accumulating far more privileges than they need to do their jobs, violating the principle of least privilege (PoLP). This may lead to inappropriate access to sensitive data that can result in poor user judgement, fraudulent changes or a data breach. Even those who should generally have elevated privileges may end up using them for nefarious goals. User rights management plays a vital role in database security by controlling which resources users can access to perform their roles and the types of actions they can perform on those resources.

The Trustwave DbProtect Rights Management module allows you to establish and monitor an environment of least privilege and monitor external and insider threats. This module provides a detailed view of your organization's data ownership, access controls, and rights to sensitive information. It allows you to establish and document compliance with the segregation of duties (SOD) controls required by industry and government regulations and reduces a formerly insurmountable task to one that is manageable. The DbProtect Rights Management software module helps organizations regain control of their user privileges and implement an effective program to adhere to the principle of least privilege.

Maintain an accurate inventory of users deployed across the enterprise

The amount of data stored on databases grows each year making them a valuable target for attack. Regulations often require evidence of strong controls over sensitive data, which makes it critical to identify and secure systems containing sensitive data. Traditionally, accurate tracking of users relied on non-automated, non-centralized solutions without any correlations between databases. It is estimated that a manual entitlement review of a typical database can take more than 80 man-hours to complete. An automated solution streamlines this process allowing organizations to discover, manage and eliminate excess permissions in a consistent manner across their heterogeneous database environment. The DbProtect Rights Management software module centralizes, automates and allows for correlation of user and role-based entitlements across databases to see the enterprise from every potential attack vector.

Meet regulatory mandates that require least privilege

In large enterprises, managing user rights ensures that appropriate data privileges have been assigned. In many organizations, rights management is a manual and reactive process typically undertaken as a requirement of a compliance audit or as a reaction to a security breach. As part of the process, the IT organization is saddled with having to identify users, examine data access and determine appropriate privileges. This is usually a manual process that significantly increases the odds of human error resulting in inaccurate findings and controls. Demonstrating effective controls to the board of directors (and the auditors) becomes a critical regulatory obligation, as shown below.

To manage these access control challenges, audit firms recommend implementing the Principle of Least Privilege, which limits access rights for employees to the minimum amount of database access required to perform their jobs. While the concept of least privilege makes perfect sense, this implementation is much more difficult than it appears. Database utilities lack appropriate reporting tools to manage least privilege implementations making entitlement reviews a complex and time-consuming process.

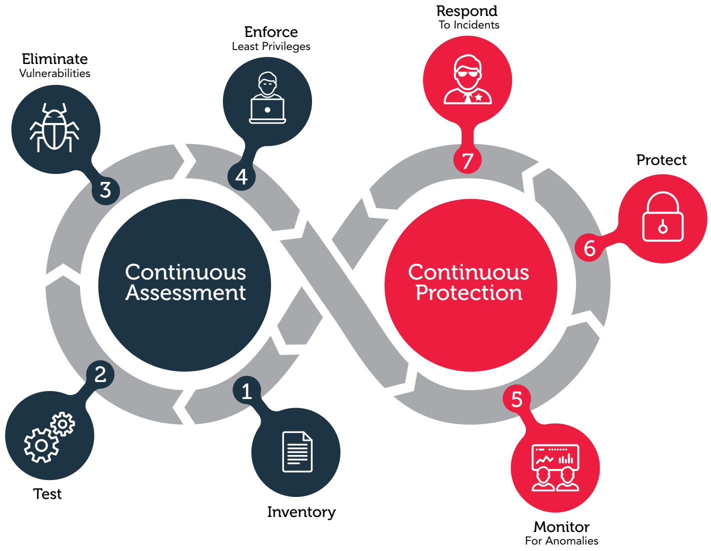
Principle of Least Privilege

Employees with inherited roles that grant a certain level of access to a database or group of database instances are often overlooked by IT and security organizations. It is often forgotten that this granular level of access control could represent a major set of vulnerabilities in the security process. As illustrated below, identifying who has permissions and how they were granted those permissions (inherited via nested roles, or granted explicitly to a user) can be an exhausting and error-prone manual exercise.

Organizations should define what constitutes appropriate access to the data. Certain users and groups of users who might be responsible for special database projects require robust levels of access while other users need permissions only for specific types of data. Defining what's appropriate and assigning privileges judiciously enables an organization to be ready to use the Principle of Least Privilege. Setting the appropriate access levels for internal employees is just as important as establishing controls for external users. Once the internal and external access policies are established and users are informed, companies need to consistently enforce these standards to prevent violations and execute on the Principle of Least Privilege.

Extending Rights Management within Enterprise Lifecycle

Part of the process in achieving continuous compliance and effectively protecting the database is ensuring that you are applying a proven lifecycle approach to security. Implementing a comprehensive database security methodology (such as the one illustrated below) ensures that organizations are implementing the best practices necessary to achieve maximum protection.



Managing user rights is enhanced by managing threats and audit-related activity relative to the database. Database activity monitoring solutions help managers monitor user and application-specific activity by delivering automated alerts if malicious or unauthorized activity occurs. Identifying and documenting users, as well as tracking effective privileges will ensure proper access controls. Having established this baseline, activity monitoring enables organizations to ensure that privileges, policies and rules are being properly used. Activity monitoring also provides a methodology to monitor internal employees who have been assigned high level privileges. A well-executed security, risk, and compliance deployment that includes vulnerability assessment, user rights review, and activity monitoring ensures an organization has the necessary steps to minimize risk and ensure compliance.

Trustwave®

For more information: www.trustwave.com