Trustwave®

DATA SHEET

# Trustwave DbProtect Rights Management

## HELP ENSURE DATABASE SECURITY BY LEAST PRIVILEGE

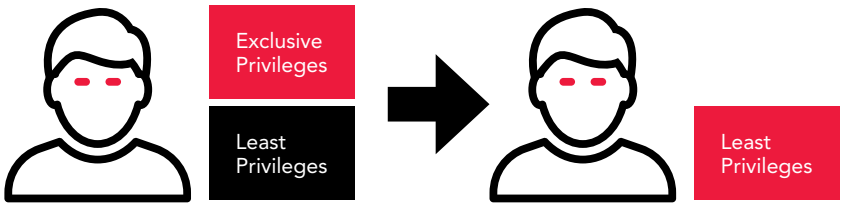
### Benefits

- Maintain an accurate inventory of database users deployed across the entire enterprise
- Identify users with inappropriate and undesired access to sensitive data
- Identify valid privileged users requiring ongoing 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.

User rights management plays a vital role in database security by controlling which resources a user can access to perform his/her role and the types of actions he/she can perform on those resources. Over time user rights can escalate and violate the principle of least privilege. Promotions, transfers, mergers and acquisition, and inheritances can result in users accumulating far more privileges than they need to do their jobs. This can lead to inappropriate access to sensitive data that can result in fraudulent changes or a data breach. Even those who should generally have privileges may end up using them for nefarious goals. For these reasons, it is imperative to establish and implement and maintain the Principle of Least Privilege (PoLP).

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 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.

### Rights Management



## The Principle of Least Privilege (PoLP)

To manage these access control challenges, audit firms recommend implementing the Principle of Least Privilege, which requires that employees be entitled only to as much database access as is necessary to perform their jobs. The concept of least privilege makes perfect sense, but, this implementation is much more difficult than it seems. Database utilities lack appropriate reporting tools to manage least privilege implementations. As a result, entitlement reviews are typically complex and time-consuming.

Streamlining this process with an automated solution allows organizations to discover, manage, and eliminate excess permissions in a manner that is consistent with effective database security process control and compliance requirements.

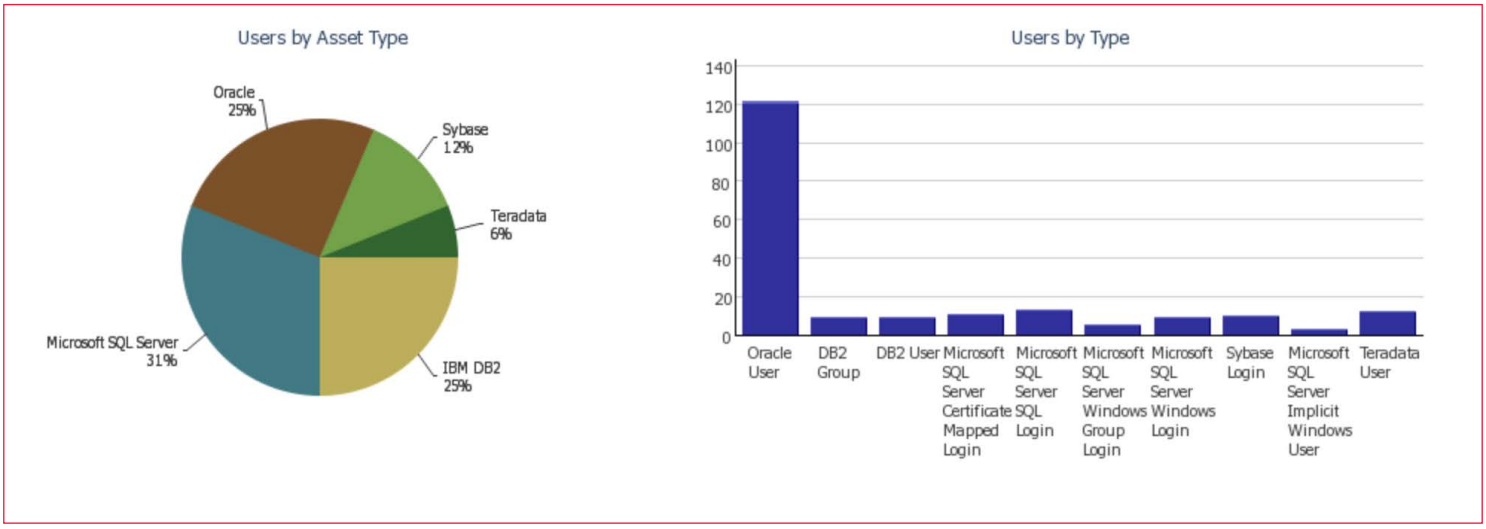



Figure1: Users by Asset Type

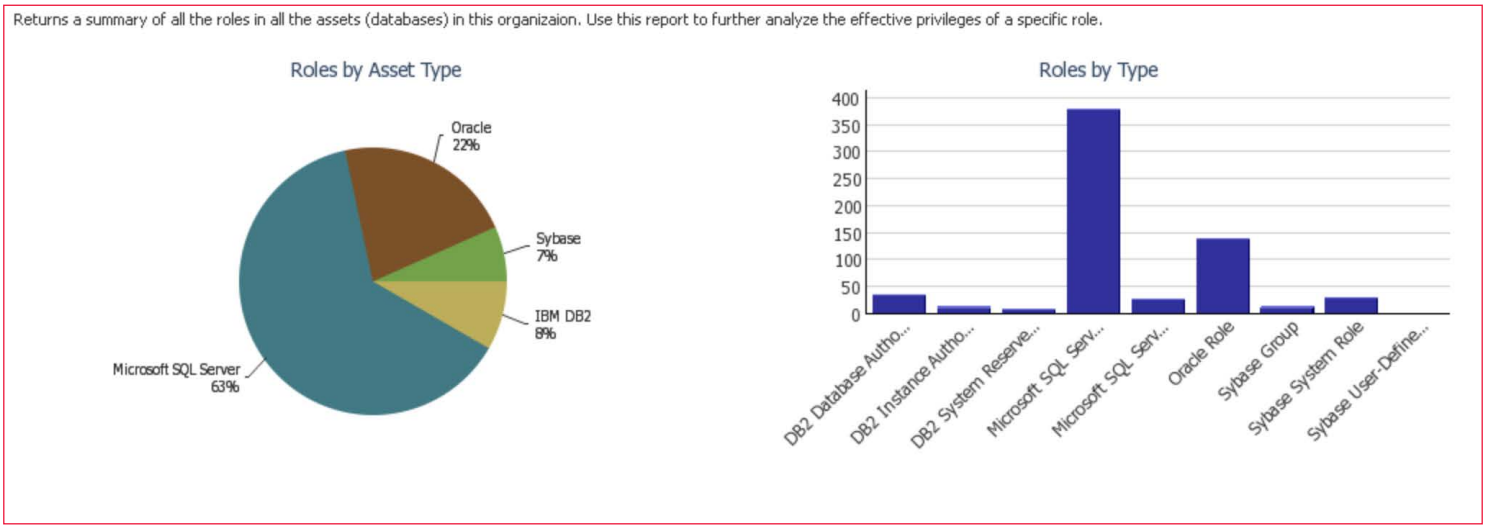



Figure2: Roles by Asset Type

Managing user privileges and monitoring for Segregation of Duties (SoD) violations are considered so important that they are defined in almost all regulatory mandates, including: Sarbanes- Oxley (SOX), PCI-DSS, NIST-800, DISA STIG, HIPAA and others.

Trustwave®

For more information: www.trustwave.com