Netwrix Auditor for Oracle Database Functionality Matrix

	Netwrix Auditor for Oracle Database	Product A	Product B
SCOPE OF COLLECTED DATA			
Change auditing Reports on changes to Oracle Database configuration and privileges, including created, modified and deleted user accounts, roles, tables, triggers, audit policies and data. Each change has information on when and where it was made, who made it, and exactly what was changed, with the before and after values.	YES		
Access auditing Monitors successful and failed attempts to log on to Oracle Database, as well as data access attempts, specifying both the account used to log on to the host OS and the Oracle Database account.	YES		
Discovery of sensitive data Finds sensitive data stored in Oracle Database so organizations can make sure that this data is not stored outside of a secure location.	YES		
SECURITY INTELLIGENCE			
Alerts on threat patterns Notifies appropriate personnel by email or SMS about critical Oracle Database activity, including single events (such as changes to Oracle Database configuration) and multiple repeated actions that has exceeded a specific threshold (such as repeated failed attempts to log on to the production database).	YES		
Behavior anomaly discovery dashboard Improves detection of malicious actors in the hybrid IT environment by delivering an aggregated trail of anomalous user activity with the associated risk scores.	YES		
User behavior and blind spot analysis reports Gives insight into potential security incidents, such as activity outside business hours or spikes in failed access attempts.	YES		
Interactive search Enables users to quickly sort through audit data and fine-tune their search criteria so they can easily hone in on the exact information they need.	YES		

Overview dashboard Shows consolidated statistics on activity across all audited databases.	YES		
Predefined reports Includes predefined audit reports that deliver detailed information about changes and access events in a human-readable format with flexible filtering and sorting options.	YES		
Custom reports Enables users to easily create custom reports on Oracle Database activity based on their specific search criteria.	YES		
Out-of-the-box compliance reports Contains ready-to-use reports tailored to specific regulatory standards, including HIPAA, PCI DSS and GDPR.	YES		
Multiple report subscription and export options Automatically delivers reports to specified recipients by email or saves them to a file share on a specified schedule. Users can export reports in multiple formats, including PDF, XLS(X), DOC(X) and CSV.	YES		
UNIFIED PLATFORM			
Enterprise-wide visibility Supports multiple IT systems and delivers cross-system visibility through dashboards and reports, both predefined and custom-built.	YES		
API-enabled integrations Can be integrated with security, compliance and IT automation tools and business applications to centralize auditing and reporting or facilitate IT workflows like change management and service desk.	YES		
Automated incident response Enables users to automate response to common and anticipated incidents by creating scripts that run each time the corresponding alert is triggered.	YES		
Reliable storage of audit data Puts the audit data into an SQL database and file storage simultaneously to reduce the risk of data loss. The audit data can be stored for more than 10 years and can be easily accessed for historic reviews and inquiries.	YES		

INSTALLATION AND CONFIGURATION			
Easy to install and configure Does not require professional services engagement or vendor assistance to fully implement the solution.	YES		
Various deployment options Offers on-premises, virtual and cloud deployment options.	YES		
Easily scalable for large enterprise environments Fits well into small and mid-size enterprises; scales seamlessly to serve large enterprises.	YES		
Role-based access control Enables granular segregation of security monitoring duties to provide each user with exactly the right access to audit data and settings.	YES		