Netwrix Auditor for Active Directory Functionality Matrix

	Netwrix Auditor for Active Directory	Product A	Product B
SCOPE OF COLLECTED DATA			
Change auditing Reports on changes to Active Directory and Group Policy, including changes to configuration and schema containers, administrative group membership, computer and user accounts, audit policies, and software settings. Each change is reported with the when, where, who and what details and the before and after values.	YES		
Logon activity auditing Shows interactive and non-interactive logon attempts, both successful and failed, as well as all logon attempts using Active Directory Federation Services.	YES		
Configuration auditing Delivers information on the configuration state of Active Directory and Group Policy, including AD account and object permissions, effective group membership, OUs, domain controllers, expired and locked user accounts, account policies, and identical settings in different GPOs.	YES		
AUDIT INTELLIGENCE			
Active Directory risk assessment Assesses risks related to improper privilege assignment and management of user and computer accounts, enabling users to remediate security gaps.	YES		
Alerts on threat patterns Notifies appropriate personnel by email or SMS about critical Active Directory activity, including single events (such as changes to the membership of a privileged group) and repeated actions that exceed a specified threshold (such as multiple failed logon attempts).	YES		

Behavior anomaly discovery dashboard Improves detection of malicious actors in the 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 logons by single user from multiple endpoints.	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 changes in Active Directory, including information on the users who made most changes, the domain controllers that are most frequently changed, the object types that are most modified and spikes in changes by date.	YES		
Predefined reports Includes predefined audit reports that deliver detailed information about changes, configuration and logon activity in a human-readable format, with flexible filtering and sorting options.	YES		
Custom reports Enables users to create custom reports on activity across Active Directory 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		
AD SPECIFIC IT MANAGEMENT FEATURES			
Change rollback and object recovery Recovers entire objects and rolls back unwanted changes without any downtime or having to restore from backup.	YES		

Inactive user tracking Reports on user and computer accounts that have been inactive for a specified number of days.	YES		
Password expiration alerting Automatically reminds users to change their passwords before they expire to ensure IT security and reduce helpdesk workload.	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 a file storage simultaneously to eliminate data loss. The audit data can be stored for more than 10 years and can be easily accessed for historic reviews and inquiries.	YES		
Non-intrusive architecture Operates without the use of agents so it doesn't degrade Active Directory performance or cause downtime.	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		