Netwrix Auditor for SharePoint Functionality Matrix

	Netwrix Auditor for SharePoint	Product A	Product B
SUPPORTED SYSTEMS AND AUDIT SCOPE			
SharePoint • Change auditing: tracking of changes made to SharePoint configurations, objects, permissions and content • Data access monitoring: reporting of document and list read access events • Access permissions reporting • Reporting on sensitive and regulated data • Support for SharePoint Foundation 2010 and 2013, SharePoint Server 2010, 2013, 2016 and 2019	YES		
SharePoint Online • Change auditing: monitoring of changes made to configurations, object, permissions and content of SharePoint Online and OneDrive for Business • Data access monitoring: reporting of user access and downloads in SharePoint Online, and file synchronization in OneDrive for Business • Access permissions reporting • Support for the version provided within Microsoft Office 365	YES		
DATA COLLECTION			
Change and data access auditing Delivers full details about changes and data access, including when and where each change or data access event was made, who made it and exactly what was changed or accessed.	YES		
Before and after values Performs full side-by-side comparisons and captures the before and after values for all modified objects.	YES		
Access permissions reporting Shows effective user permissions for specific objects within site collections, as well as how permissions were granted and whether inheritance is broken.	YES		

Reporting on sensitive and regulated data Identifies sensitive data and provides information about what types of critical data you have, where it is located, who has access to this data and how it's used. The reports work only in conjunction with Netwrix Data Classification.	YES		
Consolidated approach for hybrid IT infrastructures Collects audit data from both on-premises and cloud-based SharePoint environments, and stores it in a secure central repository, enabling unified alerting, searching and reporting.	YES		
SECURITY INTELLIGENCE			
Alerts on threat patterns Notifies appropriate personnel by email or SMS about critical SharePoint activity, including single events (such as a change to SharePoint Online configuration) and multiple repeated actions that exceed a specified threshold (such as the deletion of 100 or more files).	YES		
Behavior anomaly discovery dashboard Improves detection of malicious actors by delivering an aggregated trail of anomalous user activity across hybrid IT environments with the associated risk scores.	YES		
User profile Provides key details about each user account involved in an incident, including the name of the user, their department and manager's name, whether the account is enabled, and the AD groups it is a member of.	YES		
User behavior and blind spot analysis reports Gives insight into potential security incidents, such as activity outside business hours and non-owner mailbox access.	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 mail servers.	YES		
Predefined reports Includes predefined audit reports that deliver detailed information about changes and non-owner mailbox access in a human-readable format with flexible filtering and sorting options.	YES		

Custom reports Enables to easily create custom reports on user 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		