Netwrix Auditor for Nutanix Files Functionality Matrix

	Netwrix Auditor for Nutanix Files	Product A	Product B
SCOPE OF COLLECTED DATA			
Change auditing Reports on changes to files, folders, shares, and permissions, including the who, what, when and where details.	YES		
Read access auditing Reports on file reads, including who viewed which files and when each read event occurred.	YES		
User permissions auditing Shows effective user permissions to files and folders, as well as whether permissions were granted directly or via group membership.	YES		
Discovery and classification of sensitive data Identifies and classifies sensitive files stored on Nutanix file servers so the organizations can make sure that this data is not overexposed and that the servers with sensitive files are protected as required by internal policy and regulatory standards.	YES		
File analysis Reveals information on data ownership, data usage and data volumes, and locates empty folders and stale and duplicate files, so the organizations can effectively analyze the stored data.	YES		
SECURITY INTELLIGENCE			
Risk assessment Assesses risks related to data security, including potentially harmful files on file shares, file names that indicate they contain sensitive data and folders with permissions granted to everyone, so users can remediate security gaps.	YES		
Custom alerts on threat patterns Notifies appropriate personnel by email or SMS about critical Nutanix Files activity, including single events, such as changes to permissions, and multiple repeated actions that exceed a specific threshold, such as massive data removal.	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		
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		
Predefined reports on user permissions and file analysis Includes predefined audit reports that deliver detailed information about user permissions and file analysis in a human-readable format, with flexible filtering and sorting options.	YES		
Custom reports Enables users to easily create custom reports on Nutanix Files 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 the most common standards like HIPAA, PCI DSS, GLBA 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 custom 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 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 any intrusive services so it doesn't degrade system performance or cause downtime.	YES		
INSTALLATION AND CONFIGURATION			
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		