Netwrix Auditor for VMware Functionality Matrix

	Netwrix Auditor for VMware	Product A	Product B
SCOPE OF COLLECTED DATA			
Change auditing Reports on changes to VMware infrastructure, including hosts, containers, datacenters, resource pools, virtual machine snapshots, and virtual machines. Each change has information on when and where it was made, who made it, and what exactly was changed, with the before and after values.	YES		
Logon auditing Reports on each successful and failed logon attempt in ESXi and vCenter, including which user made the attempt and when it happened.	YES		
SECURITY INTELLIGENCE			
Alerts on threat patterns Notifies appropriate personnel by email or SMS about critical VMware events, such as deletion of a virtual machine or changes to storage resources.	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		
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 the audited VMware infrastructure.	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 VMware 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 a database and file storage simultaneously to eliminate data loss. The audit data is 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 VMware 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		