

## Netwrix Auditor for EMC Functionality Matrix

	Netwrix Auditor for EMC	Product A	Product B
<b>SCOPE OF COLLECTED DATA</b>			
<b>Change auditing</b> Reports on changes to files, folders, shares and permissions, including when and where the change was made, who made it, exactly what was changed, and the before and after values.	YES		
<b>Successful and failed access auditing</b> Reports on successful and failed file reads, showing who viewed which files and when each read event occurred.	YES		
<b>Effective permissions auditing</b> Shows effective user permissions to files and folders, as well as whether permissions were granted directly or via group membership.	YES		
<b>Discovery and classification of sensitive data</b> Identifies and classifies sensitive files stored on file servers so 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		
<b>File analysis</b> Reveals information on data ownership, data usage and data volumes, and locates empty folders and stale and duplicate files so organizations can effectively analyze their stored data.	YES		
<b>SECURITY INTELLIGENCE</b>			
<b>File server risk assessment</b> Assesses risks related to data security (including potentially harmful files on file shares, file names containing sensitive data and folders with permissions granted to everyone) to help users remediate security gaps.	YES		
<b>Alerts on threat patterns</b> Notifies appropriate personnel by email or SMS about critical file server activity, including single events (such as a change to	YES		

permissions) and multiple repeated actions that exceed a specified threshold (such as mass data removal).			
<b>Behavior anomaly discovery dashboard</b> Improves detection of malicious actors in the IT environment by delivering an aggregated trail of anomalous user activity with the associated risk scores.	YES		
<b>User behavior and blind spot analysis reports</b> Gives insight into potential security incidents, such as activity outside business hours or surges in data access.	YES		
<b>Interactive search</b> 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		
<b>Overview dashboard</b> Shows consolidated statistics on changes across all audited file servers.	YES		
<b>Predefined reports</b> Includes predefined audit reports that deliver detailed information about changes, access events, effective user permissions and file analysis in a human-readable format with flexible filtering and sorting options.	YES		
<b>Custom reports</b> Enables users to easily create custom reports on file server activity based on their specific search criteria.	YES		
<b>Out-of-the-box compliance reports</b> Contains ready-to-use reports tailored to specific regulatory standards, including HIPAA, PCI DSS, GLBA and GDPR.	YES		
<b>Multiple report subscription and export options</b> 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**

<b>Enterprise-wide visibility</b> Supports multiple IT systems and delivers cross-system visibility through dashboards and reports, both predefined and custom-built.	YES		
<b>API-enabled integrations</b> 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		
<b>Automated incident response</b> Enables users to automate response to common and anticipated incidents by creating scripts that run each time the corresponding alert is triggered.	YES		
<b>Reliable storage of audit data</b> Puts audit data into an SQL 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		
<b>Non-intrusive architecture</b> Operates without the use of any intrusive services so it doesn't degrade file server performance or cause downtime.	YES		
<b>INSTALLATION AND CONFIGURATION</b>			
<b>Easy to install and configure</b> Does not require professional services engagement or vendor assistance to fully implement the solution.	YES		
<b>Various deployment options</b> Offers on-premises, virtual and cloud deployment options.	YES		
<b>Easily scalable for large enterprise environments</b> Fits well into small and mid-size enterprises; scales seamlessly to serve large enterprises.	YES		
<b>Role-based access control</b> Enables granular segregation of security monitoring duties to provide each user with exactly the right access to audit data and settings.	YES		