

Netwrix Auditor for Network Devices Functionality Matrix

	Netwrix Auditor for Network Devices	Product A	Product B
SCOPE OF COLLECTED DATA			
Changes to the configurations of network devices Provides detailed information about who changed what on which device, and when the change was made. Includes information about configuration changes, such as changes to protocols, ports, connection limits, users and more.	YES		
Successful and failed logon attempts Reports on successful and failed attempts to log on to network devices both directly and over VPN connections, as well as successful and failed VPN logon attempts to the network.	YES		
Scanning threats Detects scanning threats and reports on which subnet and host were scanned, when each scanning attempt took place, and what IP address it was initiated from.	YES		
Hardware malfunctions Delivers information about hardware issues in network devices, including which device failed, when it failed and what caused its failure.	YES		
Supported devices Supports Fortinet FortiGate, Cisco ASA, Cisco IOS, Palo Alto, SonicWall and Juniper network devices.	YES		
SECURITY INTELLIGENCE			
Alerts on threat patterns Notifies specified personnel by email or SMS message about suspicious configuration changes and logon events, as well as about hardware issues and scanning activity, including activity that exceeds a specified baseline (threshold-based alerts).	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, such as who logged in to a particular device during the past week and what they changed there.	YES		
Predefined reports Includes predefined audit reports that deliver detailed information about configuration changes, logon attempts, scanning threats and hardware malfunctions on Cisco, Fortinet Palo Alto, SonicWall and Juniper devices in a human-readable format with flexible filtering and sorting options.	YES		
Custom reports Enables users to easily build custom reports on activity around their network devices based on their specific requirements.	YES		
Out-of-the-box compliance reports Includes ready-to-use reports that streamline preparation for PCI DSS, HIPAA, SOX, GLBA, FISMA/NIST800-53, CJIS, FERPA, NERC CIP, ISO/IEC 27001 and GDPR audits.	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 (daily, weekly, etc.). Can export reports in multiple formats, including PDF, DOCX, XLSX 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.	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 is 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		