Active Directory Auditing Solution Checklist

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Netwrix Auditor** | **Product A** | **Product B** | **Product C** |
| **DATA STORAGE AND AGGREGATION** |  |  |  |  |
| **Multi-year storage.** Utilizes a two-tiered data storage system. SQL Server for online reporting, and file-based compressed storage for long-term storage. (For greater scalability and retention of multiple years of audit data without performance degradation). | YES |  |  |  |
| **Reliable audit data.** AuditAssurance™ technology pre-filters and consolidates audit data from multiple sources including event logs, configuration snapshots, and change-history records to get a single change record for each change to provide the most reliable audit data without any gaps. | YES |  |  |  |
| **4 Ws.** Captures all changes to Active Directory including WHO made the change, WHAT was changed, WHEN it was changed (date and time), WHERE (Domain Controller) the change was made. | YES |   |   |  |
| **Before/after values.** Performs side-by-side comparison showing BEFORE and AFTER values for all modified AD Objects and settings where applicable (e.g. “Domain Admins group membership changed.”) | YES |  |  |  |
| **Leverages Native Windows Auditing** to augment the overall integrity of change information which only enables specific auditing features and does not risk generating large volumes of Event Log audit data | YES |  |  |  |
| **Protects against event log overwrites and frequent data collection** using native Windows auto-backup feature on logs | YES |  |  |  |
| **ALERTS and REPORTS** |  |
| **Reports by e-mail.** Provides daily email summary of all recent changes, sent by e-mail automatically every night to specified recipients. | YES |   |   |  |
| **Real-time alerting.** Provides real-time alerts for specific changes to AD objects by type, name, attribute name and value and does not require risky OS ‘hook’ technologies that are always running and consuming resources:* Via Email
* Via SMS
 | YESYES |  |  |  |
| **Reporting in SQL SRS.** Utilizes industry-standard SQL Server Reporting Services (free SQL Express is supported) for providing a wide selection of "out-of-the-box" [compliance-ready reports](http://www.netwrix.com/Active_Directory_Change_Reporter_Report_Samples.html). No proprietary reporting engines. | YES |   |   |  |
| **Role-based access control.** Role-based access control for reports (control who can view what reports) for administrative separation between domains, forests etc. | YES |  |  |  |
| Both web-based reporting (thin client) and Windows UI-based reporting. | YES |  |  |  |
| **Snapshot reports.** Provides ["snapshot" reports](http://www.netwrix.com/active_directory_snapshot_reports.html) of your current AD structure and enables comparing it to historical views of what it "looked" like in the past. | YES |  |  |  |
| **Report subscriptions.** Provides report –subscription capability to deliver e-mail reports to specified individuals or groups. Available attachments PDF, XLS(X), DOC(X), XML, TIFF and PDF with custom filters. (e.g. Send report about OU-level user changes to administrators responsible for that OU). | YES |   |   |  |
| **Report export.** Supports report formats: PDF, XLS(X), DOC(X), XML, TIFF, and PDF . |  |  |  |  |
| **Free custom reports.** Provides up to three custom reports at no additional cost. | YES |  |  |  |
| **Easy ad-hoc reporting** to show "Who changed what, when and where" – you just specify your managed objects (AD domains, servers, etc) and put your e-mail address and then it starts sending daily reports (e.g. every morning) so you can review each change. | YES |  |  |  |
| **Purpose-built** product for Active Directory auditing: adds human-readable formatting, not just generic raw audit data to output. | YES |  |  |  |
| **DATA COLLECTION ARCHITECTURE** |  |
| **Optional agents.** Agents may be optionally deployed but are not required and do not affect any product functionality. | YES |   |   |  |
| **No performance impact.** Agents are active at data-collection time only and do not consume server resources when not in use. | YES |  |  |  |
| **Non-intrusive.** Agents are small and non-intrusive (6k or less) and not injecting into operating system core mechanisms. | YES |  |  |  |
| Agents are used primarily for data compression. | YES |  |  |  |
| **Reliable.** Agents rely only on documented Window APIs and do not break the system when a new OS patch is released. | YES |  |  |  |
| **MANAGEMENT INTERFACE, USAGE, AND INTEGRATION CAPABILITIES** |  |
| Integrated Microsoft Management Console (MMC) interface. | YES |  |  |  |
| Integrated support for multiple forests, domains, and OUs. | YES |  |  |  |
| Supports multiple console instances for independent management. | YES |  |  |  |
| Protects existing investments by supporting “plug-in” integration with related products | YES |  |  |  |
| **ACTIVE DIRECTORY OBJECT ROLLBACK CAPABILITIES** |  |
| Easy rollback of changed objects. | YES |  |  |  |
| Object attribute-level rollback capability. | YES |  |  |  |
| Included at no additional cost | YES |  |  |  |
| **INSTALLATION, CONFIGURATION, AND PLATFORM SUPPORT** |  |
| Easy to install and configure. | YES |  |  |  |
| Can be installed with little or no vendor assistance. | YES |  |  |  |
| Does not require services engagement to fully implement. | YES |  |  |  |
| Supports 32 and 64-bit versions of Windows Server. | YES |  |  |  |
| Supports all versions of Windows Server: 2000, 2003, 2008, 2008 R2 and above without any functionality limitations. | YES |  |  |  |
| Easily scalable for large enterprise environments. Average-sized deployments of 10,000 AD users across 50 domain controllers. Largest deployments of 1 million users across 1,000 domain controllers. | YES |  |  |  |
| **INTEGRATED CONFIGURATION AUDITING FOR:** |  |   |   |  |
| **Microsoft Exchange Server** | YES |   |   |  |
| **Group Policy** (including Link Change Detection and delegated rights auditing – Create/Edit/Apply.) | YES |   |   |  |
| **Microsoft SQL Server** | YES |   |   |  |
| **File servers** (including NetApp filers and EMC Celerra) expansion module available. | YES |   |   |  |
| **SIEM add-on**: Event Log Management capabilities available. | YES |   |   |  |
| **VMware** expansion module available. | YES |   |   |  |
| **SCOM.** Microsoft-certified integration (Management Pack) with System Center Operations Manager (SCOM) enabling auditing through the SCOM console for management alerts and reporting. | YES |   |   |  |
| **SIEM Integration.** Protects investments in existing third-party SIEM platforms through integration including ArcSight Logger, IBM Tivoli, RSA enVision, Novell Sentinel, and NetIQ Security Manager | YES |  |  |  |
| **Windows servers:** Auditing for Windows servers such as software, hardware, TCP/IP, registry, local users and groups, services, scheduled tasks and more. | YES |  |  |  |