Windows Server Auditing Solution Competitive Checklist

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Netwrix**  **Auditor** | **Product A** | | **Product B** | **Product C** |
| **DATA STORAGE AND AGGREGATION** |  |  | |  |  |
| **4 Ws.** Captures all changes to server configuration including WHO made the change, WHAT was changed, WHEN it was changed (date and time), WHERE the change was made. | YES |  | |  |  |
| **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 such as when a service state changes. | YES |  | |  |  |
| **Before/after values.** Performs side-by-side comparison showing BEFORE and AFTER values for all modified settings where applicable (Ex: if a registry setting is modified, it shows the previous and new value.) | 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** using native Windows auto-backup feature on logs | YES |  | |  |  |
| **REPORTING** | | | | |  |
| **Reports by e-mail.** Provides daily email summary of all recent changes, sent by e-mail automatically every night to specified recipients. | YES |  | |  |  |
| **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" reports. No proprietary reporting engines are used or need to be learned. | YES |  | |  |  |
| Both web-based reporting (thin client) and Windows UI-based reporting. | 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 driver and hardware changes to administrators responsible for specified Windows servers). | 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 Windows Servers 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 Windows server configuration 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 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 |  | |  |  |
| Management console can be organized by logical server collections or by locations and departments, etc. | YES |  | |  |  |
| Supports multiple console instances for independent management. | YES |  | |  |  |
| Protects existing investments by supporting “plug-in” integration with other Netwrix products including integration with Netwrix Auditor | 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. | YES | |  |  |  |
| **WINDOWS SERVER CONFIGURATION CHANGE REPORTING FACILITIES FOR:** | | | | | |
| **Software** installation/removal auditing (Ex: Who removed the anti-virus software from the Exchange server?) | YES | |  |  |  |
| **Services** state change auditing (Automatic, Manual, Disabled) (Ex: Who changed the time clock service state from automatic to manual?) | YES | |  |  |  |
| **Hardware** installation and change auditing (Ex: Who installed a second NIC on the file server?) | YES | |  |  |  |
| **Scheduled tasks** change auditing (Ex: Who changed task that runs a backup routine on the accounting server from M-F to M-W-F?) | YES | |  |  |  |
| **Local User and Group change auditing** (Ex: Who added a user to the Local Administrators group on the SQL Server?) | YES | |  |  |  |
| **TCP/IP, DNS and network protocol configuration change auditing** (Ex: Who changed the DNS settings on the DC?) | YES | |  |  |  |
| **IIS** configuration change auditing (Ex: Who changed the company intranet’s site name?) | YES | |  |  |  |
| **Registry** change auditing (Ex: Who modified the registry setting that controls the use of cached logon credentials on the remote office Domain Controller?) | YES | |  |  |  |