Exchange Server Auditing Solution Competitive Checklist

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Netwrix****Auditor** | **Product A** |  **Product B** |  **Product C** |
| **DATA STORAGE** |  |  |  |  |
| **Multi-year storage:** Utilizes a two-tiered data storage system. SQL Server for online reporting, and file-based compressed storage for long-term storage (Greater scalability and can store multiple years of audit data without performance degradation). | YES |  |  |  |
| **Reliable audit data**: AuditAssurance™ technology consolidates audit data from multiple sources (event logs, configuration snapshots, change history records, etc.) to get the most reliable audit data stream without gaps. | YES |  |  |  |
| **4 Ws:** Captures all changes to Exchange including WHO, WHAT, WHEN (date and time), and WHERE (Domain Controller name), including creation and deletion of mailboxes and connectors. | YES |  |  |  |
| Supports 32 and 64-bit versions of Exchange Server. | YES |  |  |  |
| Supports all versions of Exchange Server: 2000, 2003, 2007, 2010 and 2013. | YES |  |  |  |
| **Before/after values**: Captures BEFORE and AFTER values for all modified Exchange settings (e.g. “mailbox permissions changed to include Full Access for additional users or groups”). | 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 REPORTING** |  |
| **Reports by e-mail**: Provides daily email summary of all recent changes, sent by e-mail automatically every night to specified recipients. | YES |  |  |  |
| **Easy ad-hoc reporting** to report on "Who changed what, when and where" – you just specify your managed objects (AD domains, servers, VMware 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 Exchange auditing: adds human-readable formatting, not just generic raw audit data. | YES |  |  |  |
| **Reporting in SQL SRS**: Utilizes industry-standard SQL Server Reporting Services (free SQL Express is supported) for providing a wide selection of management and compliance reports. No proprietary reporting engines. | YES |  |  |  |
| **Role-based access control** for reports (control who can view what reports) to enable administrative separation between domains, forests etc. | YES |  |  |  |
| Both web-based reporting (thin client) and Windows UI-based reporting. | YES |  |  |  |
| **Provides "reports-by-subscription"** so that any available reports can be sent via email to subscribed individuals on schedule (in attachments, e.g. PDF, XLS, DOC etc) with custom filters (e.g. send report about Exchange server setting changes to people responsible for that server). | YES |  |  |  |
| Predefined reports for compliance (HIPAA, SOX, PCI, GLBA, FISMA). | YES |  |  |  |
| Supports free version of SQL Server (SQL Express). | YES |  |  |  |
| Provides 30 predefined reports based on best practice activities and frequently changed Exchange objects, settings and permissions. | YES |  |  |  |
| **Free custom reports.** Provides up to three custom reports at no additional cost. | YES |  |  |  |
| Report formats: PDF, XLS(X), DOC(X), XML, TIFF, PDF  | YES |  |  |  |
| Enables creation of custom and ad-hoc reports via standard SQL Reporting Services mechanism (Report Builder). No need to learn proprietary vendor-specific custom report building tools. | 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 AND USAGE** |  |
| Integrated Microsoft Management Console (MMC) Interface. | YES |  |  |  |
| Supports multiple management console instances. | YES |  |  |  |
| Supports multiple Exchange Servers in multiple sites, domains, and OUs. | YES |  |  |  |
| **Integrated solution:** supports auditing of other systems and applications | YES |  |  |  |
| **INSTALLATION AND CONFIGURATION** |  |
| Easy to install and configure. | YES |  |  |  |
| Can be accomplished with little or no vendor assistance. | YES |  |  |  |
| Does not require professional services engagement to fully implement. | YES |  |  |  |
| Easily scalable for large enterprise environments. Average-sized deployment is 10,000 Exchange mailboxes across 50 Exchange servers; largest deployment is 1 million users across 500 Exchange servers. | YES |  |  |  |
| **MISCELLANEOUS FEATURES** |  |   |   |  |
| Mailbox renaming, permissions and quota change detection. | YES |  |  |  |
| Non-Owner mailbox auditing (e.g. Who is attempting to access a mailbox that may contain sensitive confidential information). | YES |  |  |  |
| Protects existing investments in 3rd-Party SIEM platforms by offering integration with SCOM, ArcSight Logger, IBM Tivoli, RSA enVision, Novell Sentinel, and NetIQ Security Manager. | YES |  |  |  |
| Protects existing investments in Netwrix products through modular integration. | YES |  |  |  |
| Provides up to three custom-built reports at no additional cost. | YES |  |  |  |