Group Policy 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 (much more scalable and can hold 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 W’s:** Captures all changes to GPOs including WHO, WHAT, WHEN (date and time), and WHERE (Domain Controller name), including creation and deletion of GPOs and links. | 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 |  |  |  |
| **Before/After Values:** Performs full side-by-side comparison and captures BEFORE and AFTER values for all modified GPO settings (e.g. “min password length changed from 12 to 7”). | 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:** Shows "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 Group Policy auditing:** adds human-readable formatting, not just generic raw audit data. | YES |  |  |  |
| **Utilizes industry-standard SQL Server Reporting Services:** (free SQL Express is supported) Provides 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 |  |  |  |
| **Report Subscriptions:** 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 OU-level GPOs to people responsible for that OU). | YES |  |  |  |
| Predefined reports for compliance (HIPAA, SOX, PCI, GLBA, FISMA). | YES |  |  |  |
| **Purpose-built** product for Active Directory auditing: adds human-readable formatting, not just generic raw audit data to output. | YES |  |  |  |
| **Report formats:** PDF, XLS(X), DOC(X), XML, TIFF, and 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 |  |  |  |
| **Free custom reports:** Provides up to three custom reports at no additional cost. | 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 forests, domains, and OUs. | YES |  |  |  |
| Supports multiple management console instances. | YES |  |  |  |
| **Integrated solution:** supports auditing of other systems and applications | YES |  |  |  |
| **BUILT-IN GPO OBJECT BACKUP/RESTORE CAPABILITIES** | | | |  |
| Restore of individual GPOs back to the original states. | 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 AD users across 50 domain controllers; largest deployment is 1 million users across 1,000 domain controllers. | YES |  |  |  |
| **MISCELLANEOUS FEATURES** |  |  |  |  |
| GPO Link Change detection. | YES |  |  |  |
| GPO Delegation Rights auditing (e.g. Create/Edit/Apply). | YES |  |  |  |
| 3rd-Party SIEM integration including SCOM, ArcSight Logger, IBM Tivoli, RSA enVision, Novell Sentinel, and NetIQ Security Manager. | YES |  |  |  |