Going Beyond Performance Visibility

As government and industry requirements continually become more stringent, Security and Compliance professionals are finding it increasingly difficult to address the myriad of monitoring and reporting details associated with data access. In particular, the financial and health care industries must safeguard client and patient data, and all organizations must proactively document many facets associated with access to IT resources.

For example, banks and credit unions in the United States operate under the **Gramm-Leach-Bliley Act (GLBA)**, which includes requirements for safeguarding sensitive data. These financial institutions must undergo regular audits by the **Federal Financial Institutions Examination Council (FFIEC)**, which consists of intensive periodic reviews of IT infrastructure and processes. A critical component of these audits includes administrative permissions, as well as the ability to monitor and document the who, what, when, where, and how associated with access to resources. Further, should a breach or questionable activity take place, it is critical that user and administrative actions have been recorded so they can be audited.

**eG Enterprise: All-in-One Solution for Performance, Security and Compliance Monitoring and Reporting**

Providing total IT performance visibility is a core focus of eG Enterprise. At the same time, since eG Enterprise monitors and documents the full array of components in virtualized infrastructures, many of the metrics collected and reported on its dashboard can be used by security and compliance professionals to fulfill requirements related to IT department procedures and configurations and for addressing government and industry requirements, as well as internal standards. Analysis of server event logs provided for detecting performance issues can also be used to track servers that have specific security flaws. Likewise, user session activity recorded for tracking the workload on a Citrix XenApp server is critical data for determining who has accessed the Citrix farm, for compliance reporting.

Many of the reports provided by eG Enterprise can assist Security and Compliance management with maintaining internal standards, as well as regulatory requirements. At no additional cost, the variety of comprehensive, built-in reports provide the security and compliance data needed with just a few clicks. Further, these reports can be output on a scheduled basis or as needed, such as when preparing for an audit.

**Security and Compliance Reporting with eG Enterprise**

**Administrative Access**

Administrative access is a primary line item for security and compliance reviews, as well as internal audit procedures. The individuals that are granted administrative access to a Citrix and/or VMware infrastructure may or may not be the same as those that have Active Directory domain admin permissions, and it is not uncommon to see vendors or partners granted some level of administrative access. As such, it is essential to ascertain exactly who has what type of administrative permissions.

---

**www.eginnovations.com**
**System Security**

System auditing is a key foundational element of security, and the disablement of auditing is often a precursor to a security breach, especially as related to a database server or other resource. Having a mechanism to track when auditing is in a state of failure can proactively identify systems that are out of compliance.

**Change Control Verification**

Change control documentation is a critical element of security and compliance reviews. Report output of the final system change, such as a new user that is provided with access to an application or resource, may be used as verification that the change control was successfully and completely executed.

**Resource Access**

Government and industry regulations address many security concerns but cannot account for all scenarios. In such cases, having a mechanism to track and monitor resources access activity that can be used for forensic purposes is critical for addressing security requirements and is typically suitable for compliance. For example, if an employee were suspected of inappropriately modifying confidential company documents, the ability to track exactly which applications were accessed and when could provide the required data points.

**Safeguarding Against Inappropriate User Activity**

Inactive user accounts are concerning because they are often overlooked by administrators but yet can be used to gain full access to resources when no longer appropriate. Regularly scheduled inactive users reports can enable Security and Compliance professionals to adhere to company and government/industry regulations.

Further, multiple failed logon and/or resource access attempts often signify inappropriate activities. The ability to track such activities is of keen interest to Security and Compliance management from a proactive standpoint as related to audits, as well as reactive forensic review.

**About eG Innovations**

eG Innovations provides intelligent performance management solutions that automate and dramatically accelerate the discovery, diagnosis, and resolution of service performance issues in virtual, cloud, and physical service infrastructures. Managing some of the largest IT deployments in the world, only eG Innovations offers 360-degree service visibility with virtualization aware performance correlation across every layer and every tier - from desktops to applications, and from network to storage. This unique approach delivers deep, actionable insights into the true causes of cross-domain service performance issues and enables administrators to pre-emptively detect, diagnose, and fix root-cause issues - before end users notice.