

# Unified Monitoring and Reporting for IT Security and Compliance

Enabling Organizational Adherence to Government/Industry Requirements and Internal Standards



## The Requirement

Security and Compliance IT professionals in many industries, particularly finance and health care, are finding it increasingly difficult to address the myriad of monitoring and reporting details associated with data access – especially with small security teams and limited budgets. What organizations need is simple and unified visibility to identify important audit events that require immediate action, so they can take remedial action.

## How eG Enterprise Helps

- ✓ Provides security and compliance professionals with easy access to actionable data so they can address complex and ever-changing government/industry regulations and internal requirements
- ✓ Reports on the who, what, when, where, and how associated with access to key IT resources
- ✓ Delivers a unified solution for performance monitoring as well as security and compliance tracking. This ensures minimal additional overhead on the IT infrastructure and simplifies deployment in the infrastructure

## 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.

Server Administrator Properties	
WIN-2011-3-2-02-b	
Privilege	Full Administration
Administrative account	Enabled
Unknown	-
Manage published applications	-
WIN-2011-3-2-02-b	
Privilege	Custom
Administrative account	Enabled
Unknown	LogOnConsole
Manage published applications	Servers: ViewSessions, ConnectSessions, SendMessages, LogOffSessions, ViewServers, TerminateProcess Applications: ViewApplications Servers/Product: ViewSessions, ConnectSessions, SendMessages, LogOffSessions, ViewServers, TerminateProcess Servers/Test: ViewSessions, ConnectSessions, SendMessages, LogOffSessions, ViewServers, TerminateProcess

## 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.

Sql Security Details	
Server authentication mode	Windows Authentication mode
Audit level	Failure
Startup service account	tengate\sv_EMEA_AXSQL

## 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.

Component Name: DPVICTXA46:1494 [Citrix XenApp 4/5/6.x] Recent changes between May 11, 2015 09:26 and Jun 11, 2015 09:26

Total Changes: 1

Component	Test	Descriptor	Measure	Previous Value	Present Value	Difference	Added
DPVICTXA46:1494: Citrix XenApp 4/5/6.x	Citrix Application Users Information	Applications/H_Tietan_Test/Update Test	Configured users	DPNT:Test01	DPNT:hyao,DPNT:Test01	DPNT:hyao,DPNT:Test01	DPNT:hyao,

## Resource Access

Government and industry regulations address many security concerns but cannot account for all scenarios. In such cases,

Session details for User - All Users

User	Session Start Time	Logout / Disconnect Time	Server	Duration Of Access (mins)	Applications	Cpu Util Avg	Memory Util Avg	Latency Avg
firm\dcruzen	06/22/2015 05:00:45	Jun 22, 2015 05:30	XA7:1494	30		0.7	4.16	0.2
firm\dcruzen	06/22/2015 04:11:31	Jun 22, 2015 04:55	XA7:1494	45		0.12	3.56	0.14
firm\dcruzen	06/21/2015 15:19:03	Jun 21, 2015 17:03	XA7:1494	104		0.29	5.4	0.45

Lists the processes executed by a user on a Citrix server

PID	PROCESS NAME	CPU(%)	MEMORY(%)	IMAGE PATH
5512	onexcul	0.1815	0.5513	C:\Program Files (x86)\Avaya\Avaya one-X Communicator\onexcul.exe
8208	winlogon	0	0.0669	winlogon.exe
9248	teamviewer	0	0.1226	C:\Program Files (x86)\TeamViewer\Version9\TeamViewer.exe
7436	explorer	0	0.3006	C:\Windows\Explorer.EXE
8552	tv_w32	0	0.0342	C:\Program Files (x86)\TeamViewer\Version9\TV\w32.exe --action hooks log C:\Program Files (x86)\TeamViewer\Version9\TeamViewer9_Logfile.l...
7532	tv_x64	0	0.0417	C:\Program Files (x86)\TeamViewer\Version9\TV\x64.exe --action hooks - log C:\Program Files (x86)\TeamViewer\Version9\TeamViewer9_Logfile.l...
11424	pdfconvservice	0	0.0465	C:\Pfx Engagement\WM\PKXPDFConvertService.exe
5904	cch.document.pdfprinter	0	0.0943	C:\Program Files (x86)\WK\ProSystem Fx Suite\Smart Client\SaaS\CCh.Document.PDFPrinter.exe
10492	sbamtray	0	0.0149	C:\Program Files (x86)\Advanced Monitoring Agent\managedav\SBAMTray.exe
7540	webformapp	0	0.0443	C:\Program Files (x86)\Common Files\STF Services Shared\WebFormApp... -start

## 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.

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.

Shows the list of inactive users			
DISTINGUISHED NAME	AGE(DAYS)	LAST LOGON	CREATED ON
Jul 06, 2015 14:34:47			
CN=Temp,OU=Temp,OU=EGE,DC=CEL,DC=EG	159	1/28/2015 4:33:35 PM	2/24/2011 3:11:23 AM
CN=test,CN=Users,DC=CEL,DC=EG	329	8/11/2014 3:10:35 PM	6/12/2014 9:32:51 AM
CN=it support,OU=Infocomm Technology,OU=Corporate Services,OU=Corporate & Enabling Services,OU=EGE,DC=CEL,DC=EG	185	1/2/2015 2:50:27 PM	7/23/2014 9:41:36 AM
CN=SP_Pool,OU=SP Service Accounts,OU=EGE,DC=CEL,DC=EG	168	1/19/2015 3:54:20 PM	1/14/2015 10:12:53 AM

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.

DATE SOURCE CATEGORY ID USER COMPUTER DESCRIPTION

Jun 04, 2015 10:42: Microsoft Windows... Logon 4625 N/A XA8 An account failed to log on. Subject: Security ID: S-1-5-10 Account Name: XA85 Account Domain: XYM Logon ID: 0x3d7 Logon Type: 2 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: craig Account Domain: XYM Failure Information: Failure Reason: Unknown user name

DATE SOURCE CATEGORY ID USER COMPUTER DESCRIPTION

Jun 10, 2015 12:56: Group Policy\Folders None 4098 NT AUTHORITY\SYSTEM XA8 The user 'Siva's' preference item in the 'GPO for Citrix XenApp (Syst Group - no redirection)' [AA054918-5C08-4635-BCB6-FBE74561A22B... e: Group Policy object did not apply because it failed with error code '0x80070005 Access is denied.'

Contact Us: [sales@eginnovations.com](mailto:sales@eginnovations.com) | [www.eginnovations.com](http://www.eginnovations.com)

US +1 866 526 6700 | SINGAPORE +65 6423 0928 | UK +44 (0)20 7935 6721 | NETHERLANDS +31 (0)70 205 5210  
INDIA +91 44 4263 9553 | LATIN AMERICA +52 55 5533 3395 | Hong Kong: +852 3972 2415